Comptes rendus mathématiques
Mathematical Reports

19

No 2

DECEMBER / DÉCEMBRE 1997

IN THIS ISSUE / DANS CE NUMÉRO

33 François Lalonde
New trends in symplectic geometry

51 Charles Helou
Cauchy-Mirimanoff polynomials

58 Georgey S. Smirnov and Roman G. Smirnov
Best Uniform Restricted Ranges Approximation of Complex-Valued Functions

64 H. Darmon
Corrigendum to Faltings plus epsilon, Wiles plus epsilon, and the Generalized Fermat Equation

C. R. Math. Rep. Acad. Sci. Canada Vol. 19 (2), 1997 pp. 33–50

NEW TRENDS IN SYMPLECTIC GEOMETRY

FRANÇOIS LALONDE

RÉSUMÉ. Je présente ici un survol des développements récents en géométrie symplectique. Cette géométrie—qu'on appelle aussi la topologie symplectique—a passé par trois moments forts au cours des quinze dernières années: les travaux de Conley-Zehnder qui l'ont enracinée dans le Calcul des Variations et la Dynamique, la percée fondamentale de Gromov qui a permis de la voir comme une généralisation très féconde de la géométrie kahlérienne, et enfin les découvertes de Seiberg-Witten et de Taubes qui ont montré la relation surprenante que la théorie quantique des champs entretient avec le symplectique, relation qui implique en particulier la coincidence entre les invariants de Seiberg-Witten (de type gauge) et ceux que Gromov construit avec les courbes holomorphes généralisées. Je décris ici les éléments de la théorie des courbes pseudoholomorphes de Gromov, les invariants qu'on en tire, les applications de cette théorie aux principaux problèmes de la géométrie symplectique. J'explique enfin comment les courbes stables—suivant une idée de Deligne et Kontsevich—peuvent servir à étendre la théorie de Gromov à toutes les variétés symplectiques. Je termine avec une courte présentation de la théorie de Taubes reliant la théorie de gauge de Seiberg-Witten à celle de Gromov.

1. Introduction. Symplectic geometry, that is the study of manifolds endowed with a symplectic form (also called "symplectic topology"), has gone through a series of revolutions during the last 15 years. The first one, initiated by Conley and Zehnder, has rooted the study of symplectic manifolds in the fields of Dynamics and Calculus of variations. More precisely, it was realised that many essential features of the theory could be related to the study of the critical points of an infinite dimensional functional—the *Action functional*—whose index and coindex are both infinite (that is to say, at each critical point, the dimensions of the positive-definite and negative-definite subspaces are infinite).

The second one due to Gromov has related Symplectic geometry to Kahler Geometry. This is done by considering a symplectic manifold as a generalised Kahler manifold—where the complex structure is not necessarily integrable—and by extending to this non-integrable case the study of the families of holomorphic curves (called in this context *pseudo-holomorphic* or *J-holomorphic*). It turns out, for deep reasons, that the topological invariants of these (finite-dimensional!) families are fine invariants of the underlying symplectic structure. Recently, ideas due to Deligne and Kontsevich have led many mathematicians to the development

Partially supported by NSERC grants OGP 0092913 and CPG0163730, and by FCAR grant ER-1199.
Received by the editors September 15, 1997.

of a theory of *stable* J-holomorphic curves that works in *all* symplectic manifolds, even untamed ones.

The third revolution, which is perhaps the most surprising, has revealed a tight relation between Symplectic geometry and Quantum physics. Note that there is obviously a close relation between Symplectic geometry and Classical physics since the former can be viewed as the framework of Hamiltonian dynamics. The relation with Quantum field theory has emerged from a totally different origin: it is Witten's and Taubes' wonderful insights that have been responsible for recognising that the Gauge theoretical Seiberg-Witten equations in QFT provide invariants of 4-dimensional manifolds that are essentially equivalent to those provided by Gromov's pseudo-holomorphic curves. In the same vein, the Quantum cohomology of symplectic manifolds, whose product structure is expressed in terms of Gromov's pseudo-holomorphic invariants, have been intensively studied recently. In some sense, Quantum cohomology is a powerful interface between QFT and Kahler geometry; for instance, it is rich enough to transform physical intuitions from QFT into precise conjectures on the number of algebraic curves passing through generic points of projective varieties!

In this survey, I wish to describe the recent developments in our understanding of symplectic geometry which are due to the progress in the theory of J-holomorphic curves. Thus I will review the recent development of stable (marked) J-curves, the relation of J-curves with Seiberg-Witten invariants and the applications of these new tools to some of the most significant problems of symplectic geometry. But before doing this, I will first quickly recall what the J-holomorphic curve approach is, why it cannot be applied to all symplectic manifolds, and why stable pseudo-holomorphic curves are needed.

2. **Preliminaries and basic facts.** A symplectic manifold is a manifold M equipped with a closed non-degenerate differential 2-form ω with real values. This means (1) that at each point $p \in M$, the form ω is a real anti-symmetric bilinear form ω_p on T_pM, which is non-degenerate in the sense that the map $v \mapsto \omega_p(v, \cdot)$ is an isomorphism from T_pM onto T^pM, and (2) that the assignation $p \mapsto \omega_p$ is smooth and its exterior derivative vanishes.

Examples of symplectic manifolds include all cotangent spaces, all Kahler manifolds (and therefore all projective varieties), and many others. For instance, using a special type of surgery that works in the neighbourhood of codimension-2 symplectic submanifolds, Gompf [5] has shown that all finitely generated groups can be realised as the fundamental group of a 4-dimensional symplectic manifold.

It turns out that the interplay between the differential condition $d\omega = 0$ and the pointwise non-degeneracy condition gives rise to a rich and subtle theory. By Darboux's theorem, any symplectic form is locally equivalent to the standard form $\sum_{1 \leq i \leq n} dx_i \wedge dy_i$ of $\mathbf{R}^{2n}$. Thus there is no local symplectic invariant, and therefore there is no hope of deriving a global invariant by integration of a local one (except the volume) . Global invariants must be constructed by other means.

One way of doing this, due to Gromov, is to consider the space of all almost complex structures compatible with the given symplectic form. Recall that an almost complex structure is any smooth assignation $p \to J_p$ where J_p is a real automorphism of the tangent space T_pM whose square is $-\mathrm{id}$ (that is to say, it makes each real $2n$-dimensional tangent space T_pM into a n-dimensional complex vector space where the multiplication by $\sqrt{-1}$ is given by application of J). It is compatible with ω if ω is J-invariant and if the form $\omega(J\cdot,\cdot)$ defines a Riemannian metric (given the J-invariance of ω, this second condition boils down to $\omega(Jv,v) > 0$ for all non-zero v). Thus each choice of a compatible almost complex structure determines a compatible Riemannian metric and conversely. Note that the three objects ω, J, g have all the features of a Kahler structure, except that J is not necessarily integrable. An almost complex structure J is integrable the complex structure that it defines on TM is induced by a complex structure on the manifold M; in other words, J is integrable if there is, near each point p, a local real diffeomorphism f onto an open set of $\mathbf{C}^n$ whose differential at each point p' sends the automorphism $J_{p'}$ of T_pM to the one on $T_{f(p')}\mathbf{C}^n = \mathbf{C}^n$ given by multiplication by $\sqrt{-1}$. On any (symplectic) manifold of real dimension at least 4, the integrable structures are rare in the space of all almost complex structures. In dimension 2, the two notions coincide.

It is very easy to see that the space $\mathcal{J}(M,\omega)$ of almost complex structures compatible with a given symplectic form is a non-empty contractible infinite-dimensional space. Now fix any such structure J. Given a Riemann surface (Σ, j) (here j denotes the complex structure, viewed as an almost complex structure) a map $u: \Sigma \to M$ is called (j, J)-holomorphic (or J-holomorphic or simply pseudo-holomorphic if there is no confusion) if the differential at each point is complex linear with respect to the structures induced by j and J. In other words, it must satisfy the generalised Cauchy-Riemann equation

$$\bar{\partial}_J u = 0$$

where $\bar{\partial}_J u \in \Lambda^{0,1}(\Sigma, u^*(TM))$ is the (j, J)-anti-complex part of du. In local coordinates, the operator $\bar{\partial}_J$ is given by

$$(\bar{\partial}_J u)(p) = \partial u/\partial y - J_p \partial u/\partial x.$$

This is an elliptic first order operator, hence Fredholm [1]. Note however that, although the equation makes sense, the operator is not yet defined globally between two Banach spaces, since the space $\Lambda^{0,1}(\Sigma, u^*(TM))$ depends on the map u. There is a trick, due to Gromov, that constructs global function spaces and some elliptic operator between them, in such a way that the zeroes of that operator are the (j, J)-holomorphic curves. It is not necessary to give here the details

[1] A linear operator between two Banach or Fréchet spaces is *Fredholm* if its image is a closed subspace of finite codimension and if the kernel is finite dimensional too. The difference dim ker − dim coker is the *index* of the Fredholm operator.

of this construction. It is more useful to explain, instead, the following equivalent construction.

Endow $\mathcal{J}$ with the C^∞-topology. This gives a Fréchet space. As explained in [23], all relevant constructions can be carried out in this C^∞ framework (although one uses in the proofs the larger Banach manifolds endowed with some Sobolev norm).

Now, for any given homology class $\alpha \in H_2(M, \mathbb{Z})$ and any non negative integer g, consider the space $\mathcal{M}_g(\alpha)$ of all non-multiply covered C^∞-maps $f\colon (\Sigma_g, j) \to (M, J)$ which are (j, J)-holomorphic and which realize the class α, where Σ_g is a real closed orientable surface of genus g, j is a (necessarily integrable) complex structure on Σ_g and J belongs to $\mathcal{J}(M,\omega)$. Here g and α are fixed but f, j and J are allowed to take any value. Thus, up to the conformal group of reparametrisations, this is the space of J-holomorphic curves of genus g in class α, for any ω-tame J. A basic fact is that the projection

$$\mathcal{P}\colon \mathcal{M}_g(\alpha) \to \mathcal{J}$$

sending f to J is essentially equivalent to the $\bar{\partial}_J$ operator (once globalised), and is therefore easily seen to be a Fredholm map between Fréchet manifolds, whose real index is $\dim_{\mathbf{R}} \mathcal{T}_g + 2(c(\alpha) - n(g-1))$. Here $\mathcal{T}_g$ is the Teichmuller space of genus g and c is the first Chern class of T_*M (note that since $\mathcal{J}$ is contractible, the Chern classes of (TM, J) do not depend on the choice of $J \in \mathcal{J}$). Thus, if J is a regular value of $\mathcal{P}$ which is in the image of $\mathcal{P}$, the space $\mathcal{M}_g(\alpha, J) = \mathcal{P}^{-1}(J)$ is a smooth manifold of real dimension equal to Index($\mathcal{P}$). When the group of conformal reparametrizations is independent of the structure j, the quotient is a manifold (of unparametrized curves) of dimension Index($\mathcal{P}$) $- \dim_{\mathbf{R}}(\mathrm{Conf}(g))$ generically. Of course, the conformal group depends on the structure j and therefore may vary from points to points in $\mathcal{M}_g(\alpha)$, but in many interesting cases the structure j which appears with the maps f is fixed by some constraints. This is of course the case for rational curves (that is those of genus 0), but also for those which are sections of irrational ruled manifolds.

For instance, in a 4-dimensional manifold M, the dimension of the unparametrized moduli space $\tilde{\mathcal{M}}_g(\alpha)$, for a class α that can be represented by an embedded real surface, is equal to $2(3g - 3 + \alpha \cdot \alpha + e_g - n(g-1) - \dim_{\mathbf{C}} \mathrm{Conf}(g))$ where e_g is the Euler characteristic of Σ_g. This is because the Chern number of α is the sum of the Euler characteristics of the tangent and normal bundles, and in the embedded case, the latter is equal to the self-intersection of the surface.

Of course, the interest in considering these moduli spaces is that any embedded J-holomorphic curve is necessarily *symplectic* in the sense that the restriction of ω to that surface is non-degenerate. Actually, it is easy to see that, conversely, given any smooth embedded symplectic surface S, there is a compatible J such that S becomes J-holomorphic, and one can moreover choose that J to be generic with respect to any other property.

Finally, let me mention that as in algebraic geometry, there is also here a compactness theorem which forms, with the positivity of intersection, the cornerstone of the holomorphic approach:

THEOREM 2.1. *Let (M,ω) be a geometrically bounded symplectic manifold and $f_i: (\Sigma_g, j_i) \to (M, J_i)$, $i \geq 1$, a sequence of holomorphic maps of fixed genus g such that:*

1) the images of the maps f_i all lie in some compact set of M,

2) the sequence $\{J_i\}$ belongs to a compact set K, and

3) there exists an upper bound A on the ω-areas of the curves:

$$\int_{\Sigma_g} f_i^* \omega \leq A \quad \text{for all } i \geq 1.$$

Then there exists a subsequence weakly converging to a J-cusp-curve, for some $J \in K$.

See [1] for a precise definition of geometric boundedness (which depends on the data (M,ω,J)). Any compact manifold or any cotangent bundle is geometrically bounded, and this property is stable under products. See [23, 1] for the definition of cusp-curves and weak convergence. In the ambient space M, this theorem essentially means that the curves C_i (the image of f_i, that we may consider as singular 1-dimensional complex submanifolds) converge to a connected union of J-curves, one of which has genus g and all other having genus 0 (these rational curves are produced by bubbling off). A particular case of this theorem is that any moduli space $\tilde{\mathcal{M}}_g(\alpha, J)$ has a natural compactification. The question is then: does this compactification assign to $\tilde{\mathcal{M}}_g(\alpha, J)$ a boundary of dimension less than the dimension of $\tilde{\mathcal{M}}_g(\alpha, J)$? If yes, can this be used to define natural cycles? Can one derive symplectic invariants from these cycles?

The answers to these questions have first been given in the context of *weakly monotone* symplectic manifolds. This is where the so-called Gromov invariants were first defined (see below). More recently, these constructions have been generalised to all symplectic manifolds, thanks to Deligne and Kontsevich [10, 11] idea of extending to the symplectic case the stack construction in algebraic geometry. This gave rise to the theory of *virtual stable marked pseudo-holomorphic curves*, that I will explain in the next sections.

3. **Gromov's invariants.** The simplest application of pseudoholomorphic curves in symplectic geometry is the construction of the Gromov (or Gromov-Witten) invariants. They are invariants of the symplectic structure, defined in the following way. Let α be any homology class in $H_2(M,\mathbf{Z})$ and k a non-negative integer. Fix a generic structure J and consider the evaluation map

$$\text{ev}: \tilde{\mathcal{M}}_0(\alpha, J) \times_G (S^2 \times \ldots \times S^2) \to (M \times \ldots \times M)$$

defined by $\mathrm{ev}(u, z_1, \ldots, z_k) \mapsto (u(z_1), \ldots, u(z_k))$, where $G = \mathrm{PSL}(2, \mathbf{R})$ is the reparametrization group acting in the obvious way on both factors and $\times_G$ denotes the quotient by this diagonal action. Now given homogeneous homology classes $\alpha_1, \ldots, \alpha_k$ in $H_*(M, \mathbf{Z})$, one can form their product in $H(M, \mathbf{Z}) \otimes \ldots \otimes H(M, \mathbf{Z}) \equiv H(M \times \ldots \times M, \mathbf{Z})$, take a representative of it which is transversal to ev and finally take the inverse image by ev. With the index fomula for pseudo-holomorphic curves, it is easy to compute the dimensions of the cycles α_i so that this inverse image be 0-dimensional. When, moreover, the inverse image is independent of all choices (J, representatives of α_i) and defines a compact oriented 0-cycle, one gets an invariant by counting these points with appropriate signs. This will be the case as soon as the image of the evaluation map defines a geometric object in $M \times \ldots \times M$ which shares all the properties of a compact oriented cycle, except that one allows boundaries of codimension at least 2 (over $\mathbf{R}$). Following McDuff-Salamon [23], let's call this a *pseudo-cycle*. The main result of this section is that the Gromov compactness theorem implies that the image of the evaluation map always defines a pseudo-cycle when the symplectic manifold (M, ω) is *weakly monotone.*

DEFINITION. A symplectic manifold (M, ω) is *weakly monotone* if, given any compatible J, there is no rational J-holomorphic curve in homology classes α with Chern index $-2n + 3 \leq c_1(\alpha) < 0$

THEOREM 3.2. *In a weakly monotone manifold, the image of the evaluation map always defines a pseudo-cycle. Thus the Gromov invariants are well-defined in this case.*

Before explaining what is the problem with non weakly monotone manifolds and how it has been solved, let me first review other applications of pseudo-holomorphic curves, which are especially interesting from a geometric point of view.

4. **Foliations by J-holomorphic curves.** There are many other applications of pseudo-holomorphic curves to symplectic and contact geometry. For instance, these curves have been extensively used in the series of papers [16, 17, 18] by Lalonde-McDuff to prove the Non-squeezing theorem for all symplectic manifolds and to develop a new intrinsic geometry of the infinite dimensional group of Hamiltonian diffeomorphisms of a symplectic manifold introduced by Hofer in 1990 [6] (called *Hofer's geometry*). See [15] for a review of these results. Another example is the application by Eliashberg and Hofer of pseudo-holomorphic curves to 3-dimensional contact geometry. A *contact structure* on a 3-manifold V is a maximally non-integrable distribution of 2-planes. If the distribution is expressed as the kernel of a 1-form α, this means that $\alpha \wedge d\alpha$ nowhere vanishes. In other words $d\alpha$ is non-degenerate on the kernel of α. The *Reeb flow* is the vector field X defined as the kernel of $d\alpha$ (which is therefore transversal to $\ker d\alpha$) and such

that $\alpha(X) = 1$. In order to attach fine invariants to the contact structure or to study the behaviour of the Reeb foliation on V, one fruitful approach is to embed $V = V \times \{1\}$ in its *symplectization* $M = V \times (0, \infty)$ endowed with the symplectic form $d\alpha + \alpha \wedge dz$. It turns out that, in some cases, the periodic orbits of X can be found as the boundary of pseudo-holomorphic discs in M (see Hofer [7]). There is actually a tight relation between the properties of pseudo-holomorphic curves in the symplectization and the properties of the Reeb flow. The development of this method has led to the definition of a new homology, called contact homology, which encodes some of the most subblte invariants of the contact structure (this work is ongoing, a full definition of contact homology has not yet appeared, except very recently in a combinatorial way in a preprint by Chekanov [2]).

Since any 3-manifold admits a contact structure, there is some (speculative) hope that a symplectic program could eventually be developped in order to study three-dimensional geometry. In this vein, Thurston and Eliashberg have recently collaborated on the development of a theory tha would unify contact structures and two-dimensional foliations, called the theory of *confoliations*. Similarly, Hofer and Wisocki have recently shown that the three-sphere admits a characterization purely in terms of dynamical properties of the Reeb flow [9].

As a last example of applications of J-curves, I wish to describe briefly their use in the classification of *rational* and *ruled* symplectic 4-manifolds. This terminology refers to the complex geometry of surfaces: a rational manifold is diffeomorphic to the projective plane, and a ruled one is diffeomorphic to a S^2-bundle over a closed oriented real surface. The clasification is then the following. Recall first that a minimal manifold is one that cannot be expressed as the blow-up of another manifold: in complex terms, this means that it does not contain an exceptional divisor, and in symplectic terms this means that it does not contain an embedded symplectic 2-sphere of self-intersection -1.

THEOREM 4.3 (GROMOV, TAUBES). *On a manifold diffeomorphic to* $\mathbf{CP}^2$, *any symplectic structure is equivalent to the standard Fubini-Study structure.*

The proof of this theorem relies both on the theory of J-curves as developped by Gromov in [4] and on the equivalence, due to Taubes, of Gromov's and Seiberg-Witten's invariants [28](see below).

THEOREM 4.4 (GROMOV, LALONDE-MCDUFF). *On a manifold diffeomorphic to a S^2-fibration, any symplectic structure is equivalent to a standard Kahler one (and is therefore classified by the cohomology class of the form).*

Here is a sketch of the main steps of the proof for the case when M is diffeomorphic to $\Sigma_g \times S^2$, where Σ_g is the surface of genus g (there is of course also a topologically non-split S^2-fibration over Σ_g, but the proof in that case is similar to the case when the underlying manifold is topologically split). See [19] for details.

(1) First, one finds a symplectic 2-sphere of self-intersection 0 by first constructing a solution to the Seiberg-Witten equations and then using Taubes' equivalence between these invariants and Gromov invariants (see §7 below). This shows that there is a non-vanishing Gromov invariant attached to the class of the S^2-fiber and consequently there is at least one J-holomorphic 2-sphere in the class of the fiber, for a generic J. This gives the required symplectic 2-sphere of self-intersection 0.

(2) For generic J, consider the moduli space of unparametrised rational J-curves in the class F of the fiber. By a regularity criterion (see [8]) similar to the one given by the Riemann-Roch in the complex case, the differential of the Fredholm projection is everywhere onto along the points in $\mathcal{M}_0(F, J)$, so that this moduli space (which is non-empty by (1)) is a smooth real manifold of dimension 2. The Gromov compactness theorem then gives a description of the degenerations that may arise if that space is not compact. A careful study of these accidents (which consists of bubbling off leading to the decomposition of the curve into two or more components) shows that they connot happen for generic J's. Hence one easily derives from this that the manifold M is actually foliated by smooth embedded J-holomorphic spheres in class F.

(3) Suppose that the base of the fibration M were a sphere instead of a surface of genus $g = 2$. Then the same argument as in steps 1 and 2 would show that the class B of the flat sections of the fibration $M \to S^2$ is foliated by ω-symplectic 2-spheres too. We would then have two foliations, one for each S^2-direction. This would give a diffeomorphism f from $S^2 \times S^2$ to itself which would send the straight S^2-coordinates to the curved ones. Denote by $\omega_{st} = \omega_0 \oplus \omega_1$ the standard split symplectic form on $S^2 \times S^2$, where each ω_i is the standard area form on S^2 whose area is the same as the integral of ω on that same factor (hence at the cohomology level $[\omega] = [\omega'])$. Denote by ω' the pushforward of this split symplectic structure by f. Then, by construction, the two foliations considered above are ω-symplectic as well as ω'-symplectic. This implies that J is compatible with both ω and ω' and therefore that the segment $\omega_t = \lambda\omega' + (1-\lambda)\omega, \lambda \in [0, 1]$, between them is formed of non-degenerate forms, hence of symplectic forms in the same cohomology class as $[\omega] = [\omega']$. There is a basic theorem of symplectic geometry, due to Moser and whose proof is elementary, which states that such a segment is necessarily induced by a diffeotopy $\phi_{t\in[0,1]}$ in the sense that $\phi_t^*(\omega_t) = \omega$. Hence $\phi_1^*(\omega') = \omega$, which shows that ω is equivalent to ω'. This is the line of the argument when the base has genus 0. Such an argument breaks down in genus > 0 because the index formula readily implies that a generic J never admits a foliation of $\Sigma_g \times S^2$ by J-curves of genus g. The argument in genus > 0 is actually completely different.

(4) Let's go back to the general case of genus g. The idea is to reduce the proof to the case of genus 0. For this, we consider a wedge of $2g$ circles Λ on Σ_g which cuts Σ_g into a $4g$-polygon, and all intersect at the point $x \in \Sigma_g$ say. The inverse

image of each such circle γ_i by the projection $\pi: M \to Si_g$ is a hypersurface H_i of M. It is well-known that the restriction of a symplectic form to any hypersurface always has at each point a kernel of dimension 1 (this is an easy exercise of linear algebra). In particular, each hypersurface H_i has such a vector field called *characteristic flow*, which is necessarily transversal to the S^2-fibers of π since the form is non-degenerate on each such fiber. This induces a flow, and therefore a monodromy (or one turn map)

$$R_i: S^2 \to S^2$$

where here S^2 is the fiber F_x over the point x, and the map is defined by beginning at a point $p \in S^2$ and flowing along the characteristic flow till one comes back to the same fiber. This map is actually a symplectic diffeomorphism of S^2 and therefore is Hamiltonian. It is now very easy to convince oneself that, if all maps $R_i, 1 \leq i \leq 2g$ were the identity, then the form ω would be equivalent to a split form. Indeed, in this case, up to diffeomorphism one can arrange that the form be split near $\pi^{-1}(\Lambda)$. But then, by cutting the manifold along $\pi^{-1}(\Lambda)$, one gets a form on a the product $P \times S^2$ of a polygon and a sphere, which is split near the boundary. After identification of the boundary with a single fiber, one gets a manifold ruled over the sphere, and by (3) our symplectic form is known to be equivalent to a standard split one. Since this equivalence can be made to be the identity near a fiber where the form is already split (relative case), this shows that the equivalence on $S^2 \times S^2$ can be carried to an equivalence between ω and a split form ω_{split} on the space $P \times S^2$ and finally on the original space M.

(5) There remains the critical step: how to show that our form ω on M is equivalent to a form that makes all the monodromies trivial? Note first that by the theorem of normal forms near a symplectic manifold, the form ω can be considered split near the fiber F_x, that is on a neighbourhood of the form $D \times S^2$ where D is a small disc centered at x. Now the first observation is that, if the form ω is deformed so that the area it gives to the disc D becomes sufficiently large (without changing the form in the vertical direction of the fiber), then one gets enough place to perturb each hypersurface so that the monodromy R_i becomes trivial. Note that the perturbation needed here can a be arbitrarily large; this is why this step requires a large deformation of ω, which obviously changes the cohomology class of ω. This is proved using the geometric properties of Hofer's geometry. It is a purely symplectic step where pseudoholomorphic curves do not intervene. See [19] for details.

(6) Putting the last steps together gives a deformation of the symplectic structure from the original form to a split form: the first one from $\omega = \omega_{t=0}$ to $\omega_{t=1/3}$ is a deformation that changes the cohomology class, it joins the original form ω to a form where all monodromies R_i are trivial. The second deformation is actually an isotopy, it joins the form $\omega_{1/3}$ to a standard split form $\omega_{2/3} = \omega_{split}$. Of course,

we can add finally a deformation inside the space of split forms between $\omega_{2/3}$ and a split form ω_1 in the same cohomology class as ω. Let's denote by $\omega_{t\in[0,1]}$ this whole deformation. In this last step, I describe how to change a deformation ω_t of the symplectic form, whose ends ω_0 and ω_1 are in the same cohomology class, into a genuine isotopy ω'_t joining the same ends. This means that the image $[\omega'_t]$ of ω'_t in $H^2(M, \mathbf{R})$ is a single point. Actually, it is enough to require that the classes $[\omega'_t]$ belong to the line L of $H^2(M, \mathbf{R})$ passing through 0 and $[\omega_0] = [\omega_1]$ because a rescalling of each form takes them back to a single point and therefore defines a genuine isotopy.

This is a rather more elaborate step, so I will have to describe this in a very sketchy way. The basic observation is that if S is a symplectic surface in a 4-dimensional symplectic manifold, then the symplectic structure near the surface has a canonical form which is adapted to the Thom class of the normal bundle of S in the sense that there is a representative Φ of that Thom class such that $\omega + \tau\Phi$ is a symplectic form *for all* $\tau \geq 0$ (this can be expressed by saying that the Thom class is the *normal factor* of the symplectic form). Hence the existence of a t-family of ω_t-symplectic surfaces S_t in a given homology class α enables one to change the path ω_t to a path $\omega'_t = \omega_t + \tau_t PD(\alpha)$ where τ_t is any smooth positive function of t. Note here that we only need two such classes. Indeed, as I said above, it is enough to transform ω_t into a deformation ω'_t whose classes $[\omega'_t] \in H^2(M, \mathbf{R}) \equiv \mathbf{R}^2$ all lie on the line L of $H^2(M, \mathbf{R})$. But in order to do this, we only need to deform ω_t in a direction L_t of $H^2(M, \mathbf{R})$ whose slope is respectively less than the slope of L if $[\omega_t]$ lies above L, or greater than the slope of L if $[\omega_t]$ lies under L (note that $[\omega_t]$ alway lies in the first quadrant of $H^2(M, \mathbf{R})$). One finally gets the existence of these two classes by showing that both the class F of the fiber and the class $n_1 B + n_2 F$ (for any sufficiently large ratio n_1/n_2) have non-zero Gromov invariants. As before, this is proved by showing that the Seiberg-Witten invariants corresponding to these classes do not vanish. ∎

5. **The negative multiple curve problem.** As I explained in the last section, many of the most significant problems of symplectic geometry depend on the "good behaviour" of pseudo-holomorphic curves in symplectic manifolds. This is why the Gromov invariants, the Floer homology and other similar tools were first defined only when this behaviour is tamed, that is when the manifold is weakly monotone. It is time to explain what the problem is when the manifold is not weakly monotone. Consider a class $\alpha \in H_2(M'\mathbf{Z})$ such that $c(\alpha)$ is negative but larger than $-2n + 1$, and assume that that class admits J-rational representatives for generic J. Assume moreover that α is not a primitive class, say $\alpha = 2\beta$, and suppose that β too contains J-rational representatives. The compactification of $\mathcal{M}_0(\alpha, J)$ is formed of all reducible curves whose components are multiple branched coverings of some rational curves, with the obvious constraint that the homology class realised by the sum of the components (counting multiplicities)

is equal to α. In particular, the boundary of the compactification contains the double covering of any J-rational curve C in class β. But a simple count, using the index formula, shows that the dimension of the moduli space of β-rational-J-curves is greater than the dimension of the moduli space of α-rational-J-curves (this actually is obvious since the Chern index appears with positive sign in the index formula). Hence, in this situation, the boundary of the compactified moduli space has a dimension greater than its "interior", so that one is incapable of defining in such a case any sensible notion of (pseudo-) cycle through any evaluation map. For reasons slightly more subbtle, the same problem prohibits the application of J-curves to the definition of Floer homology or to a direct proof of the Non-squeezing theorem.

To solve this problem, one is led to deform the $\bar{\partial}_J$ equation in some "virtual way".

6. **Virtual stable pseudoholomorphic curves.** Deligne and Kontsevich have noted that the notion of stack in algebraic geometry should have an analogue in the smooth category that would apply to all symplectic manifolds. This program, that solves the negative multiple curve problem, has been conducted simultaneously and independently by many mathematicians, namely Fukaya-Ono [3], Ruan [25], Hofer-Salamon (unwritten yet) and Liu-Tian [14] with slightly different approaches. We will describe here Liu-Tian's approach. They are all based on the notion of *(marked) stable pseudoholomorphic curves.*

A stable J-holomorphic cusp-curve is defined in the following way. First, we denote by $\mathcal{M}_{g,k}$ the moduli space of Riemann surfaces of genus g with k marked points, assuming that $2g + k \geq 3$. Each point of that space can be presented as $(\Sigma, x_1, \ldots, x_k)$ where Σ is a Riemann surface and the k points are distinct. Two such objects are identified whenever there is a biholomorphism sending marked points to marked points. Denote by $\bar{\mathcal{M}}_{g,k}$ the Deligne-Mumford compactification of $\mathcal{M}_{g,k}$. Thus it consists of all *stable* maps with k points, that is to say a connected Riemann surface whose worst singularities are ordinary (transversal) double points, with total genus g (the total genus is the genus of the surface obtained by index 1 surgery on the double points) and k marked points with the condition that, on each component Σ_i of this connected union, the relation $2g_i + k_i \geq 3$ be always satisfied, where this time k_i is the sum of the numbers of singularities and marked points of the i^{th}-component. It is moreover required that the graph formed by the components of the curve is a tree. Two such objects are identified in the obvious way, by biholomorphisms that respect both the singularities and the marked points. The main motivation for this definition is that a stable curve only admits a *finite* group of automorphisms

Finally, the J-holomorphic stable maps are J-holomorphic maps defined on the connected Riemann surfaces $\Sigma = \cup\Sigma_i$ with the weaker restriction that the relation $2g_i + k_i \geq 3$ is needed only when the restriction of the map to that component is a "ghost" (sent to a point). There is an obvious notion of equivalence, and the quotient is the moduli space $\bar{\mathcal{F}}_{g,k}(M)$ of *stable maps*. Again the automorphism group is finite. Denoting by $\bar{\mathcal{F}}_{g,k}(M,\alpha)$ the same space with the additional condition that the maps realise the homology class $\alpha \in H_2(M)$, we get as an easy consequence of Gromov's compactness theorem:

THEOREM 6.5. *$\bar{\mathcal{F}}_{g,k}(M,\alpha)$ is both Hausdorff and compact.*

Now the basic idea is to use the finiteness of the automorphism group to construct an orbifold structure on the space of J-holomorphic stable maps. Once this is done, we perturb the $\bar{\partial}_J$ equation by adding an inhomogeneous term, depending on the stable map, in such a way that the multiple curve problem desappears (note that this problem is due to the fact that a covering of a J-holomorphic cuve is also a J-holomorphic curve, but that propery is killed when such a perturbation is introduced). The new "virtual stable maps" are then the solution of this non-homogeneous equation. One can then show that they behave well in *all* symplectic manifolds in the sense that the give rise to evaluation maps—naturally associated to the marked points—which do define pseudo-cycles, at least if one uses rational coefficients.

7. Seiberg-Witten equations and Taubes' theory. In 1994, Seiberg and Witten found a system of elliptic PDE's, of gauge theoretical nature, when they were investigating the consequences of a certain supersymmetric quantized Yang-Mills theory [26, 27]. Witten realised that this system of equations would greatly simplify Donaldson-Taubes's theory of instantons as invariants of the differential structures of 4-manifolds (see [29]). Indeed, the replacement of the Yang-Mills equations by the SW-equations leads to a theory that is essentially as rich as the Donaldson one, but with the enormous advantage that the space of solutions to the SW-equations already forms a *compact* set in most cases. The SW-equations have already led to

(1) a reformulation and simplification of Donaldson's theory;

(2) a proof of the Thom conjecture on the minimal genus of a smooth embedding of a real closed oriented surface that realises a given homology class of dimension 2 in $\mathbf{CP}^2$ (the conjecture states that it should be equal to the genus of the faithful holomorphic curve in the given class); extension of the proof to many other 4-manifolds, the so-called manifolds of non-simple type (see [12]);

(3) the proof of the Theorems 4.3 and 4.4 above;

(4) many applications to the classification of *tight* contact structures (the tight contact stuctures, introduced by Eliashberg at the end of the 80's, are essentially the structures that behave in a rigid way; they are opposed to the *overtwisted* contact structures that behave in a way that is prescribed by purely topological considerations). See [22, 13, 24]

Here is in a few words a summary of Seiberg-Witten's theory, as presented in Lalonde-McDuff [19].

From their definition, it is clear that the Gromov invariants of (M, ω) depend only on the deformation class of ω. Taubes's main result is that they coincide with certain Seiberg-Witten invariants and so depend only on the smooth structure of M together with the first Chern class $c_1(J)$ of any ω-tame almost complex structure J. We must state his result somewhat carefully since ruled surfaces have $b_2^+ = 1$, which means that the Seiberg-Witten invariants depend both on the metric and the perturbation used to define them. Normally we will consider metrics of the form g_J defined by

$$g_J(x, y) = \omega(x, Jy),$$

where here we assume that J is ω-compatible, ie that $\omega(Jv, Jw) = \omega(v, w)$ as well as $\omega(v, Jv) > 0$.

To be consistent with usual notation we denote by K the complex line bundle with first Chern class $-c_1(\omega)$ and let E be a complex line bundle whose Chern class $c_1(E)$ is denoted $e \in H^2(M, \mathbf{Z})$. Given such E let W_E denote the Spin^c-structure on M with determinant bundle $L_E = K^{-1} \otimes E^2$. The (perturbed) Seiberg-Witten equations on W_E may be written as

$$D_A(\Phi) = 0, \quad F_A^+ = \sigma(\Phi) - i\eta, \tag{1}$$

where F_A^+ is the self-dual part of the curvature of a connection A on L_E, σ is a quadratic function of the spinor Φ, and η is a real self-dual 2-form. The number of solutions of equations (1) (counted with sign) is independent of the choice of J and η as these vary along a generic path (J_t, η_t) provided that this path does not cross the "wall" where there are reducible solutions. (These are solutions with $\Phi = 0$, which pose problems because the gauge group does not act freely at such points.) Because $[iF_A] = 2\pi c_1(L_E)$ and because $\omega \wedge \alpha \equiv 0$ for all antiselfdual forms α, such reducible solutions occur exactly when

$$2\pi c_1(L_E) \cup [\omega] = [\eta] \cup [\omega].$$

Taubes considers perturbations of the form

$$\eta_r = 4r\omega + iF_{A_0}^+, \quad r \to \infty,$$

where A_0 is the connection on K^{-1} which is defined by g_J. We define $\mathrm{SW}_K(L_E)$ to be the number of solutions of equations (1) for some fixed (large) value of r. It is not hard to see that this invariant is well-defined and independent of ω up to deformation. Moreover, Taubes's theorem can be stated in this language as

$$\mathrm{SW}_K(L_E) = \pm \mathrm{Gr}\,(PD(e)).$$

Therefore, in order to conclude our survey of the classification of (rational or irrational) ruled symplectic 4-manifolds, it is enough to show that $\mathrm{SW}_K(L_E)$ is nonzero for classes e which are Poincaré duals of homology classes $A = m[F] + n[\Sigma]$ with either $n = 0$ and $m = 1$ or n/m arbitrarily large. Here $[F]$ is the class of the fiber and $[\Sigma]$ is the class of the section. As observed by Li-Liu and Ohta-Ono, this can be done by using a wall-crossing formula. The point is that ruled surfaces always have metrics g of positive scalar curvature, and it is well-known that the unperturbed Seiberg-Witten equations have no solutions in this case. Further, the number of times that a path from the pair $(g, 0)$ to a Taubes pair (g_J, η_r) crosses the wall is 1 (when counted with multiplicities). Therefore, provided that the wall-crossing number (that is the jump in the number of Seiberg-Witten solutions) is nonzero for the class e, the Taubes invariant $\mathrm{SW}_K(L_E)$ will be nonzero. Note that this is possible only when the formal dimension of the Seiberg-Witten solution space is ≥ 0. When $e \in H^2(M)$ is Poincaré dual to A, this dimension is exactly the number $2k(A) = c_1(A) + A \cdot A$ which occurs in the definition of the Gromov invariant.

By calculating this wall-crossing number, one shows:

PROPOSITION 7.6 (LI-LIU, OHTA-ONO). *Let (M,ω) be a symplectically ruled surface over Σ where $g = \mathrm{genus}\,(\Sigma) > 0$, and let $e \in H^2(M, \mathbf{Z})$ be Poincaré dual to $A = m[F] + n[\Sigma]$, where the fiber class $[F]$ and base $[\Sigma]$ are as defined in §3. Then, if $k(A) \geq 0$,*

$$\pm \mathrm{Gr}\,(A) = \mathrm{SW}_K(L_E) = (n+1)^g.$$

8. **Topological rigidity of Hamiltonian loops.** As a last application of virtual stable pseudoholomophic curves, let me describe briefly the surprising phenomenon of topological rigidity of Hamiltonian loops, discovered recently by Lalonde-McDuff-Polterovich [21].

Consider the following question: is the group of Hamiltonian diffeomorphisms C^1-closed in the group of symplectic diffeomorphisms (or equivalently in the full group of all diffeomorphisms)? This has been studied in the paper [20]. In order to explain some of the results therein, let's recall that the flux of a path of symplectic diffeomorphisms $\phi_t, t \in [0,1]$, beginning at the identity, is given by integrating over time the ω-dual of the time-dependent vector field that generates the path. Since the path is symplectic, this dual is necessarily closed, as well as its integral, which therefore defines a class in $H^1(M, \mathbf{R})$, called the flux of ϕ_t, which turns out to be independent up to homotopy of the path that keeps its endpoints (id and ϕ_1) fixed. Another definition of the flux is the assignation to ϕ_t of the element of $H^1(M, \mathbf{R})$ defined as the composition

$$H_1(M, \mathbf{Z}) \overset{\partial_\phi}{\to} H_2(M, \mathbf{Z}) \overset{\int \omega}{\to} \mathbf{R}$$

where the first map is simply given by $\gamma(s) \mapsto \phi_t(\gamma(s))$, which we will refer to as the *trace* on γ of $\phi(t)$ (this trace obviously makes sense as a map from $H_i(M, \mathbf{Z}) \to H_{i+1}(M, \mathbf{R})$ for any i). Since the dual of the trace map behaves like a derivation, we will sometimes call ∂_ϕ a *derivation*. An essential algebraic ingredient in this study is the image of the Fux homomorphism $\pi_1(\mathrm{Diff}_\omega(M)) \to H^1(M, \mathbf{R})$ where the Flux is defined as above (using either definition). We will denote by Γ this image, called the Flux subgroup. Then the basic facts needed can be expressed in the following way:

1 Suppose that a symplectic diffeomorphism is given as the endpoint of a symplectic path $\phi_t, t \in [0,1]$. Then ϕ_1 is Hamiltonian if and only if the flux of the path ϕ_t belongs to the subgroup $\Gamma \subset H^1(M, \mathbf{R})$. That is to say the knowledge of Γ is the essential ingredient in order to decide if a given symplectic diffeomorphism is Hamiltonian.

2 The group of Hamiltonian diffeomorphisms is C^1-closed in the group of symplectic diffeomorphisms if and only if the subgroup $\Gamma \subset H^1(M, \mathbf{R})$ is discrete (in the sense that each element γ of Γ is included in some open neighbourhood of $H^1(M, \mathbf{R})$ whose intersection with Γ contains only γ). Clearly, discreteness is equivalent to the fact that Γ be topologically closed in $H^1(M, \mathbf{R})$. This (discreteness or C^1-closure) is known as the Flux conjecture.

Putting this together, and using both soft and hard methods, we established in [20] that the Flux conjecture holds in many cases, for semi-monotone manifolds for instance or spherically rational ones. We feel that we have enough evidence to state, as a conjecture, that the Flux conjecture should hold in all closed symplectic manifolds. It is however much more speculative to decide whether or not the C^0-flux conjecture (stating that $\mathrm{Diff}_{\mathrm{Ham}}(M)$ is C^0-closed in the identity component of the group of symplectic diffeomorphisms) is true in general. In [20], we were only able to establish this for a special class of manifolds including tori. This seems a crucial question of symplectic topology: as in the case of Eliashberg's C^0-closedness of the group symplectic diffeomorphisms that prompted the development of the theory of capacities, the C^0-closedness of the group of Hamiltonian diffeomorphisms is related to the extent to which the C^0-invariants of Hamiltonian paths (like Floer homology) are genuinely attached to Hamiltonian diffeomorphisms.

In our study of the C^1-flux conjecture, we were led to a related problem. To explain this, consider a closed symplectic manifold (M, ω) and a loop $\phi_{t\in[0,1]}$ of symplectic diffeomorphisms based at the identity. Then the homotopy class of that loop contains a Hamiltonian loop exactly when the composite map

$$H_1(M, \mathbf{R}) \xrightarrow{\partial_\phi} H_2(M, \mathbf{R}) \xrightarrow{\int \omega} \mathbf{R}$$

described above vanishes. When it vanishes, we say that the loop $\phi_{t\in[0,1]}$ is *Hamiltonian up to homotopy* (or even simply *Hamiltonian* by abuse of terminology). Thus, a priori, the fact that the loop be Hamiltonian up to homotopy seems to depend heavily on the choice of the symplectic form. We showed in [21] that this is not the case:

THEOREM 8.7 (LALONDE-MCDUFF-POLTEROVICH). *Let (M,ω) be a closed symplectic manifold and $\phi_{t\in[0,1]}$ be a loop based at the identity in the group* $\mathrm{Diff}_\omega(M)$ *of symplectic diffeomorphisms. Then, if the flux of that loop vanishes, the trace map itself*

$$H_1(M,\mathbf{R}) \overset{\partial_\phi}{\to} H_2(M,\mathbf{R})$$

vanishes. Actually, all trace maps

$$H_i(M,\mathbf{R}) \overset{\partial_\phi}{\to} H_{i+1}(M,\mathbf{R})$$

vanish. In other words, all trace maps vanish for elements of $\pi_1(\mathrm{Ham}(M))$.

This theorem has the following obvious corollary:

COROLLARY 8.8 (TOPOLOGICAL RIGIDITY OF HAMILTONIAN LOOPS). *Let M be a closed manifold, and $\gamma \in \pi_1(\mathrm{Diff}(M))$. Suppose that this loop has ω_i-representatives, $i = 1,2$, for symplectic forms ω_1 and ω_2 on M. Then the first representative is Hamiltonian (up to homotopy) if and only if the second is.*

This topological rigidity implies the following *Hamiltonian stability*: given an element ϕ_t in $\pi_1(\mathrm{Ham}(M,\omega))$ generated say by closed 1-forms λ_t, any other symplectic form ω' (that can belong to a different cohomology class) obviously gives rise to a ω'-path beginning at the identity, by integrating the ω'-dual of the closed 1-forms λ_t. But if ω' is sufficiently close to ω, the endpoint of the new path is C^1-close to the identity and therefore can be joined to the identity using the theory of generating 1-forms. This gives a ω'-loop in the same homotopy class of loops in $\mathrm{Diff}(M)$. Hence, by the theorem, the trace map must also vanish, which implies that this new loop is also Hamiltonian (up to homotopy)!

COROLLARY 8.9 (HAMILTONIAN STABILITY). *Let ϕ_t be a Hamiltonian loop with respect to some symplectic form ω. There is a neighbourhood of ω in the space of symplectic forms and, for each ω' in this neighbourhood, there is a loop ϕ'_t in the same homotopy class of loops which is Hamiltonian with respect to ω'. The correspondance $\omega' \mapsto \phi'_t$ can be made continuous.*

Here is finally the relation between the topological rigidity of Hamiltonian loops and the Flux conjecture:

COROLLARY 8.10. *The rank over $\mathbf{Z}$ of the group*

$$H_\omega = \pi_1(\mathrm{Diff}_\omega(M))/\pi_1(\mathrm{Ham}(M))$$

(which is identified with Γ by the Flux homomorphism) is not greater than the first Betti number of M. In particular, it is finitely generated over $\mathbf{Z}$.

PROOF. Suppose not, then there are symplectic loops $\phi_1, \ldots, \phi_m$ with $m > \beta_1(M)$ independent over $\mathbf{Z}$, mod $\pi_1(\mathrm{Ham}(M))$. Thus their fluxes λ_i must also be independent over $\mathbf{Z}$ in $H^1(M, \mathbf{R})$. Perturb the form ω to a rational form ω' and do the same for the new loops and fluxes (denoting them with a prime symbol). Recall that this can be done so that the new loops are in the same homotopy classes in Diff(M) as the former ones. Since the new fluxes are rational, there is a non-trivial integral linear combination of them $\lambda' = \Sigma_i n_i \lambda'_i$ that vanishes, and therefore by the Main theorem, the loop $\phi' = \Pi_i(\phi'_i)^{n_i}$ has trivial derivation. Thus the corresponding loop $\phi = \Pi_i(\phi_i)^{n_i}$ has also trivial derivation and must a fortiori have trivial flux. But this means that the loop is in $\pi_1(\mathrm{Ham}(M))$, a contradiction with the hypothesis. ∎

COROLLARY 8.11. *The Flux conjecture holds when the first Betti number of* M *is* 1.

REFERENCES

1. M. Audin and J. Lafontaine (eds), *Holomorphic curves in symplectic geometry.* Progress in Mathematics **117**, Birkauser, 1994.
2. Y. Chekanov, preprint, 1997.
3. K. Fukaya and K. Ono, *The Gromov invariants and Arnold conjecture.* preprint, 1996.
4. M. Gromov, *Pseudo-holomorphic curves in symplectic manifolds.* Invent. Math. **82** (1985), 307–347.
5. R. Gompf, *Some new symplectic 4-manifolds.* 1992.
6. H. Hofer, *On the topological properties of symplectic maps.* Proc. Royal Soc. Edinburgh **115 A** (1990), 25–38.
7. H. Hofer, *Pseudoholomorphic curves in symplectizations with applications to the Weinstein conjecture in dimension three.* Invent. Math. **114** (1993), 515–563.
8. H. Hofer, V. Lizan, J.-C. Sikorav, *On genericity for holomorphic curves in 4-dimensional almost-complex manifolds.* J. Geom. Anal., to appera.
9. H. Hofer and K. Wysocki, *A dynamical characterization of the 3-sphere.* preprint.
10. M. Kontsevich, *Enumeration of rational curves by torus actions, in Moduli spaces of surfaces.* H. Djikgraaf, C. Faber and G. V. D. Geer eds, Birkhauser, 1995, 335–368.
11. M. Kontsevich and Y. Manin, *Gromov-Witten classes, Quantum cohomology and enumerative geometry.* Comm. Math. Phys. **164** (1994), 525–562.
12. P. Kronheimer and T. Mrowka, *The genus of embedded surfaces in the projective plane.* Math. Res. Letters **1** (1994), 797–808.
13. P. Kronheimer and T. Mrowka, *Monopoles and contact structures.* preprint, 1996.
14. G. Liu and G. Tian, *Virtual moduli cycles and Gromov-Witten invariants of general symplectic manifolds.* preprint, 1996.
15. F. Lalonde, *Energy and capacities in symplectic topology.* AMS/IP Studies in Advanced Mathematics **2** (1997), 328–374.
16. F. Lalonde and D. McDuff, *The geometry of symplectic energy.* Ann. of Math. **141** (1995), 349–371.
17. F. Lalonde and D. McDuff, *Hofer's L^∞-geometry: energy and stability of Hamiltonian flows, I and II.* Invent. Math. **122** (1995), 1–34 and 35–70.
18. F. Lalonde and D. McDuff, *Local Non-Squeezing theorems and stability.* J. Geom. Funct. Anal. **5** (1995), 364–386.
19. F. Lalonde and D. McDuff, *The classification of ruled symplectic 4-manifolds.* Math. Res. Lett. **3** (1996), 769–778.

20. F. Lalonde, D. McDuff and L. Polterovich, *On the Flux conjectures.* to appear in the Proceedings of the CRM Workshop on Geometry, Topology and Dynamics, ed. F. Lalonde, Montreal 1995, to be published in the special CRM Series of the AMS.
21. F. Lalonde, D. McDuff and L. Polterovich, *The topological rigidity of Hamiltonian loops.* preprint, 1997.
22. P. Lisca and G. Matic, *Tight contact structures and the Seiberg-Witten invariants.* preprint, 1996.
23. D. McDuff and D. Salamon, *J-holomorphic curves and quantum cohomology.* AMS University Lecture Series, vol. 6, American Mathematical Society, 1994.
24. T. Mrowka and P. Ozsvath, B. Yu, *Seiberg-Witten monopoles on Seifert fibered spaces.* preprint, 1996.
25. Y. Ruan, *Virtual neighbourhoods and pseudo-holomorphic curves.* Preprint alg-geom/9611021.
26. N. Seiberg and E. Witten, *Electromagnetic duality, monopole condensation and confinement in $N = 2$ supersymmetric Yang-Mills theory.* Nucl. Phys. **B426** (1994), 19–52.
27. N. Seiberg and E. Witten, *Monopoles, duality and chiral symmetry breaking in $N = 2$ supersymmetric QCD.* Nucl. Phys. **B431** (1994), 581–640.
28. C. Taubes, *From the Seiberg-Witten equations to pseudo-holomorphic curves.* J. Amer. Math. Soc. 9 (1996), 845–918.
29. E. Witten, *Monopoles and four-manifolds.* Math. Res. Lett. 1 (1994), 769–796.

Université du Québec à Montréal
flalonde@math.uqam.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 19 (2), 1997 pp. 51–57

CAUCHY-MIRIMANOFF POLYNOMIALS

CHARLES HELOU

Presented by M. Ram Murty, F. R. S. C.

RÉSUMÉ. Les polynômes $P_n = (X+1)^n - X^n - 1$, de Cauchy, ont des facteurs cyclotomiques simples. Mirimanoff conjectura que le facteur restant, E_n, est irréductible sur $\mathbb{Q}$. Le groupe de Galois de E_n est déterminé par ceux de polynômes auxiliares. Sur un corps fini $\mathbb{F}_p$, E_n est réductible si n est impair; mais pour N premier, on déduit du nombre de facteurs sur $\mathbb{F}_p$ un critère d'irréductibilité sur $\mathbb{Q}$. Enfin, si p est premier, E_{2p} est irréductible sur $\mathbb{Q}$.

1. **Introduction.** For any integer $n \geq 2$, let $P_n(X) = (X+1)^n - X^n - 1$ and let E_n be the remaining factor of P_n, in $\mathbb{Q}[X]$, after removing X and the cyclotomic factors. Then

$$(1) \qquad P_n(X) = (X+1)^n - X^n - 1 = X(X+1)^{\epsilon_n}(X^2+X+1)^{e_n}E_n(X)$$

where for even n, $\epsilon_n = e_n = 0$; for odd n, $\epsilon_n = 1$ and $e_n = 0, 1$ or 2 according as $n \equiv 0, 2$ or $1 \pmod 3$. Cauchy noted (1) for odd n in 1839 ([2,3,6]). Mirimanoff studied E_n for prime n in 1903 ([4]) and conjectured its irreducibility over $\mathbb{Q}$. Most of his results are valid for all odd n and his conjecture seems to hold for all $n \geq 2$. Moreover, for odd $n \geq 9$, E_n is reducible modulo every prime p. For prime n, if E_n has at most 3 irreducible factors modulo some prime p then it is irreducible over $\mathbb{Q}$. Also for odd n, the Galois group of E_n over $\mathbb{Q}$ is an extension of a subgroup of $\mathfrak{S}_3^{r_n}$ by a subgroup of $\mathfrak{S}_{r_n}$; and presumably it is the wreath product of $\mathfrak{S}_3$ by $\mathfrak{S}_{r_n}$, where $\mathfrak{S}_k$ is the symmetric group on k letters and $r_n = \frac{n-3-2e_n}{6}$. This is reminiscent of some results of P. Morton on the Galois group of periodic points of polynomial maps ([5]). Another generalization of Mirimanoff conjecture ([7]), and several other helpful ideas, were suggested by G. Terjanian. The irreducibility of E_{2p}, for odd prime p, is due to M. Filaseta.

2. **Preliminary results.** For any integer $m > 0$, let $\zeta_m = e^{\frac{2i\pi}{m}}$ in $\mathbb{C}$. Then ζ_3 is a root of P_n if $n \equiv \pm 1 \pmod 6$; and so is -1 if n is odd. These are the only roots of unity that are roots of P_n. Indeed, if $m \geq 4$ and $n \geq 3$ then $|(\zeta_m + 1)^n| = (2\cos\frac{\pi}{m})^n > 2 \geq |\zeta_m^n + 1|$. Moreover, P_n has no other real roots

Reçu par les éditeurs le March 7, 1997.
AMS subject classification: 11C08, 11R09, 11R32.

than 0 and (if n is odd) -1, since P_n' has at most one root in $\mathbb{R}$. A multiple root x of P_n is characterized by $(x+1)^{n-1} = x^{n-1} = 1$, whose solutions in $\mathbb{C}$ are $x = \zeta_3^j$ $(j = 1, 2)$ provided $n \equiv 1 \pmod 6$. The multiplicity of a root is ≤ 2, since P_n, P_n' and P_n'' have no common root. Therefore $X^2 + X + 1$ is a simple or double factor of P_n according as $n \equiv -1$ or $1 \pmod 6$. Hence the factorization in (1), with E_n in $\mathbb{Z}[X]$ having only simple roots in $\mathbb{C}$, none of which is real nor a root of unity. Moreover, E_n is, like P_n, a reciprocal polynomial, i.e. if $E_n(X) = \sum_{k=0}^{d_n} a_k X^k$ with d_n its degree then $a_{d_n-k} = a_k$ $(0 \leq k \leq d_n)$. Thus, if x is a root of E_n then so are its complex conjugate $\bar{x}$ and its inverse $\frac{1}{x}$. Note also that if n is prime, then $\frac{1}{n}E_n$ is a monic polynomial in $\mathbb{Z}[X]$, whose roots are then algebraic integers.

LEMMA 1. *For $n \geq 2$, E_n has at least $2\nu_n$ roots of absolute value 1 in $\mathbb{C}$ with $\nu_n = [\frac{n}{6}] - 1$ if $n \equiv 1 \pmod 6$, $\nu_n = [\frac{n}{6}]$ otherwise and $[x]$ the largest integer $\leq x$.*

PROOF. $P_n(e^{i\theta}) = 2w_n(\frac{\theta}{2})e^{\frac{in\theta}{2}}$, where, for $x \in \mathbb{R}$, $w_n(x) = 2^{n-1}\cos^n x - \cos nx$. Thus, $e^{\pm i\theta}$ are roots of E_n if and only if $\frac{\theta}{2}$ is a zero $\neq \frac{\pi}{3}$ of w_n in $(0, \frac{\pi}{2})$. For integers $\frac{n}{3} \leq k \leq \frac{2n}{3} - 1$, the continuous function w_n has opposite signs at the endpoints of $[\frac{k\pi}{n}, \frac{(k+1)\pi}{n}]$ and thus has a zero in this interval. Moreover $w_n(\pi - x) = (-1)^n w_n(x)$, and $w_n(\frac{\pi}{2}) = 0$ if and only if n is odd. Hence w_n has ν_n zeros in $(\frac{\pi}{3}, \frac{\pi}{2})$.

We assume until §4 that n is odd ≥ 9. Then $E_n(-X-1) = E_n(X)$ and $E_n(\frac{1}{X}) = \frac{1}{X^{d_n}}E_n(X)$. Hence, if z is a root of E_n in $\mathbb{C}$, then so are the elements of

$$\text{(2)} \qquad \operatorname{Orb}(z) = \{z, \frac{1}{z}, -z-1, -\frac{1}{z+1}, -1-\frac{1}{z}, -\frac{z}{z+1}\}$$

which are distinct, since $z \neq 1, -2, -\frac{1}{2}, \zeta_3, \zeta_3^2$. This set is the orbit of z under the action of the group of unimodular transformations $\mathcal{T} = \{X, \frac{1}{X}, -X-1, -\frac{1}{X+1}, -\frac{X+1}{X}, -\frac{X}{X+1}\}$ on $\mathbb{C} - \{0, -1\}$. The group $\mathcal{T}$ is isomorphic to $\mathfrak{S}_3$. The roots of E_n in $\mathbb{C}$ are thus partitioned into $r_n = \frac{d_n}{6} = \frac{n-3-2e_n}{6}$ orbits. In every orbit, there are at most two elements of absolute value 1, namely z and $\frac{1}{z}$, since $z^2 + z + 1 \neq 0$. Moreover $r_n = \nu_n$ of Lemma 1. Hence

LEMMA 2. *For odd $n \geq 9$, the roots of E_n in $\mathbb{C}$ are partitioned into r_n orbits (2); and E_n has exactly $2r_n$ roots of absolute value 1, two conjugates in each orbit.*

For every root z of E_n in $\mathbb{C}$, let g_z be the monic polynomial with roots the elements of $\operatorname{Orb}(z)$. A straightforward computation gives

$$\text{(3)} \qquad g_z(X) = X^6 + 3X^5 + t_z X^4 + (2t_z - 5)X^3 + t_z X^2 + 3X + 1$$

with $t_z = 6 - J(z)$ and $J(X) = \frac{(X^2+X+1)^3}{X^2(X+1)^2}$. The definition and expression of g_z are valid for any $z \in \mathbb{C} - \{0, -1\}$ and we have

$$\text{(4)} \qquad g_z(X) = X^2(X+1)^2(J(X) - J(z)).$$

All elements in $\mathrm{Orb}(z)$ have the same image by J. If $\theta \not\equiv \pi \pmod{2}\pi$, in $\mathbb{R}$, then $J(e^{i\theta}) = \frac{(2\cos\theta+1)^3}{2(\cos\theta+1)}$. So, if z is a root of E_n, then $J(z) \in \mathbb{R}$ and $g_z \in \mathbb{R}[X]$. The roots of E_n being partitioned into r_n orbits, E_n is the product of the corresponding polynomials g_z, with leading coefficient n. Thus

LEMMA 3. *For odd $n \geq 9$, if $z_1, \ldots, z_{r_n}$ are representatives of the root orbits of E_n in $\mathbb{C}$, then $E_n = n\prod_{j=1}^{r_n} g_{z_j}$, with $g_{z_j} \in \mathbb{R}[X]$ given by (3). For a root z of E_n, $t_z = 6 - J(z)$ is a real algebraic number; if n is prime, it is an algebraic integer.*

Let T_n be the monic polynomial with roots $t_j = t_{z_j}$, i.e. $T_n(X) = \prod_{j=1}^{r_n}(X-t_j)$. Then $T_n \in \mathbb{Q}[X]$; if n is prime, $T_n \in \mathbb{Z}[X]$. For, the automorphisms of $\mathbb{C}$ permute the roots of E_n hence of T_n and thus fix its coefficients. By Lemma 3 and (4),

$$E_n(X) = (-1)^{r_n} n X^{2r_n}(X+1)^{2r_n} T_n(6 - J(X)). \tag{5}$$

It follows that if E_n is irreducible over $\mathbb{Q}$, then so is T_n.

3. Some Galois groups. For odd $n \geq 9$, let $z_j = e^{i\theta_j}$ $(1 \leq j \leq r_n)$ be representatives of the root orbits of E_n in $\mathbb{C}$. Write $t_j = t_{z_j} = 6 - J(z_j)$ and $g_j = g_{z_j}$. Let $K = \mathbb{Q}(t_1, \ldots, t_{r_n})$ and $L = \mathbb{Q}(z_1, \ldots, z_{r_n})$ be the splitting fields of T_n and E_n over $\mathbb{Q}$. Note that $K \subset \mathbb{R}$. Let $G = \mathrm{Gal}(L|\mathbb{Q})$, $N = \mathrm{Gal}(L|K)$, $G_K = \mathrm{Gal}(K|\mathbb{Q})$ be the Galois groups of $L|\mathbb{Q}$, $L|K$, $K|\mathbb{Q}$. For $\sigma \in G$ and $1 \leq j \leq r_n$, the root $\sigma(z_j)$ of E_n is in the orbit of some z_k $(1 \leq k \leq r_n)$, i.e. $\sigma(z_j) = R_{\sigma,j}(z_{\pi_\sigma(j)})$ with $R_{\sigma,j} \in \mathcal{T}$, $\pi_\sigma(j) = k$. Then $\sigma(t_j) = t_{\pi_\sigma(j)}$ and $\pi_\sigma \in \mathfrak{S}_{r_n}$. The map $\sigma \mapsto \pi_\sigma$ is a homomorphism from G into $\mathfrak{S}_{r_n}$ with kernel N and image $\simeq G_K$. It identifies G_K with a subgroup $\mathfrak{H}$ of $\mathfrak{S}_{r_n}$, i.e. $G/N \simeq \mathfrak{H}$. Also, for $\sigma, \sigma' \in G$, we have $R_{\sigma'\sigma,j} = R_{\sigma,j}R_{\sigma',\pi_\sigma(j)}$ $(1 \leq j \leq r_n)$. This relation may be interpreted as defining an element of $H^1(\mathfrak{H}, \mathfrak{S}_3^{r_n})$, class of a 1-cocycle $\pi \mapsto (R_{\tau_\pi,j})_{1\leq j\leq r_n}$, where $\tau_\pi \in G$ is any extension to L of the element of G_K corresponding to $\pi \in \mathfrak{H}$. Thus

PROPOSITION 1. *For odd $n \geq 9$, any $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ is given by $\sigma(z_j) = R_{\sigma,j}(z_{\pi_\sigma(j)})$, $\sigma(t_j) = t_{\pi_\sigma(j)}$, where $R_{\sigma,j} \in \mathcal{T}$, $\pi_\sigma \in \mathfrak{S}_{r_n}$ $(1 \leq j \leq r_n)$. The map $\sigma \mapsto \pi_\sigma$ induces an isomorphism between $\mathrm{Gal}(K|\mathbb{Q})$ and a subgroup $\mathfrak{H}$ of $\mathfrak{S}_{r_n}$. And $\mathrm{Gal}(L|\mathbb{Q})$ is an extension of $\mathrm{Gal}(L|K)$ by $\mathfrak{H}$.*

Since $L|K$ is the compositum of $K(z_j)|K$, lifting by K of $\mathbb{Q}(z_j)|\mathbb{Q}(t_j)$ $(1 \leq j \leq r_n)$, we consider

LEMMA 4. *Let n be odd ≥ 9 and z a root of E_n in $\mathbb{C}$.*

a) We have $\mathbb{Q}(z) \cap K = \mathbb{Q}(t_z)$ and $\mathrm{Gal}(K(z)|K) \simeq \mathrm{Gal}(\mathbb{Q}(z)|\mathbb{Q}(t_z)) \simeq \mathcal{T}_z$, where $\mathcal{T}_z$ is a subgroup of $\mathcal{T}$ of order $|\mathcal{T}_z| = 2$ or 6.

b) For a $\mathbb{Q}$-conjugate z' of z, $\mathcal{T}_{z'} = \mathcal{T}_z$. The minimal polynomial of z over $\mathbb{Q}$ is the product of $[\mathbb{Q}(t_z) : \mathbb{Q}]$ minimal polynomials over K of such z' in different orbits.

c) If $|\mathcal{T}_z| = 2$ then, for any $z'' \in \mathrm{Orb}(z)$, $|\mathcal{T}_{z''}| = 2$; and, if $|z| = 1$ then all the roots of the minimal polynomial of z over $\mathbb{Q}$ have absolute value 1.

PROOF. a) Let u_z be the minimal polynomial of z over $\mathbb{Q}(t_z)$, $\mathcal{T}_z$ the set of $R \in \mathcal{T}$ such that $R(z)$ is a root of u_z and $G_z = \mathrm{Gal}(\mathbb{Q}(z)|\mathbb{Q}(t_z))$. Any $s \in G_z$ is characterized by $s(z) = R_s(z)$ with $R_s \in \mathcal{T}_z$. If s is the restriction to $\mathbb{Q}(z)$ of some $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ and $z = R(z_j)$ with $1 \leq j \leq r_n$ and $R \in \mathcal{T}$, then $\pi_\sigma(j) = j$ and $\sigma(z_j) = R_{\sigma,j}(z_j)$, so that $R_s = RR_{\sigma,j}R^{-1}$. Hence the isomorphism $s \mapsto R_s^{-1}$ from G_z onto the subgroup $\mathcal{T}_z$ of $\mathcal{T}$. Also, $|\mathcal{T}_z|$ is the degree of u_z and divides $|\mathcal{T}| = 6$. Since $u_z \in \mathbb{R}[X]$ has no real roots, its degree is even and is thus 2 or 6. Let $K_z = \mathbb{Q}(z) \cap K$; then $H_z = \mathrm{Gal}(\mathbb{Q}(z)|K_z)$ is a normal subgroup of G_z with $|H_z|$ even. But $|G_z| = 2$ or 6, and in the latter case $G_z \simeq \mathfrak{S}_3$. Thus $H_z = G_z$, i.e. $K_z = \mathbb{Q}(t_z)$ and $\mathrm{Gal}(K(z)|K) \simeq G_z \simeq \mathcal{T}_z$.

b) Let U_z be the minimal polynomial of z over $\mathbb{Q}$, and z' a root of U_z. For $R \in \mathcal{T}$, $R(z')$ is a root of U_z if and only if there is a field isomorphism τ_R from $\mathbb{Q}(z)$ onto $\mathbb{Q}(z')$ such that $\tau_R(z) = R(z')$. In this case, $\tau_R(t_z) = t_{z'}$, and $s = \tau_1^{-1}\tau_R$ is in G_z and satisfies $s(z) = R(z)$, so that $R \in \mathcal{T}_z$. Similarly, $\tau_R\tau_1^{-1} \in G_{z'}$, so that $R \in \mathcal{T}_{z'}$. It follows that $\mathcal{T}_z = \mathcal{T}_{z'}$ and the roots $R(z')$ of $u_{z'}$ are those of U_z that lie in $\mathrm{Orb}(z')$. Hence U_z is the product of $u_{z'}$ for z' taken in different orbits. Since $[K(z') : K] = [\mathbb{Q}(z') : \mathbb{Q}(t_{z'})]$, $u_{z'}$ is also the minimal polynomial of z' over K. The degree of $u_{z'}$ is $|\mathcal{T}_{z'}| = |\mathcal{T}_z| = [\mathbb{Q}(z) : \mathbb{Q}(t_z)]$. The result follows.

c) Let $|\mathcal{T}_z| = 2$ and $z'' \in \mathrm{Orb}(z)$. Then $t_{z''} = t_z$ and $u_{z''}$ is a factor of $g_{z''}$ of degree 2 or 6. If it was 6, then $u_{z''} = g_{z''} = g_z$, implying $u_z = g_z$, a contradiction. Thus $|\mathcal{T}_{z''}| = 2$. If $|z| = 1$, i.e. $\bar{z} = \frac{1}{z}$, then $u_z(X) = (X - z)(X - \frac{1}{z})$; and for a root z' of U_z, $\mathcal{T}_{z'} = \mathcal{T}_z$ implies $u_{z'}(X) = (X - z')(X - \frac{1}{z'})$, so that $\overline{z'} = \frac{1}{z'}$, i.e. $|z'| = 1$.

COROLLARY 1. *In $\mathbb{Q}[X]$, if T_n is irreducible, then E_n is either irreducible or is the product of 3 irreducible factors (according as g_z is irreducible over $\mathbb{Q}(t_z)$ or not).*

PROOF. U_z is the product of r_n polynomials $u_{z'}$, irreducible over K, all of degree $d = 6$ or 2. So U_z is an irreducible factor of E_n in $\mathbb{Q}[X]$ of degree dr_n. If $d = 6$, i.e. $g_z = u_z$, then $E_n = U_z$ is irreducible over $\mathbb{Q}$. Otherwise, U_z and every $U_{z''}$, for $z'' \in \mathrm{Orb}(z)$, have degree $2r_n$ so that E_n has 3 irreducible factors.

COROLLARY 2. *For odd $n \geq 9$, $\mathrm{Gal}(L|\mathbb{Q})$ is an extension of a subgroup of $\mathfrak{S}_3^{r_n}$ by a subgroup of $\mathfrak{S}_{r_n}$.*

PROOF. L is the compositum of the fields $K(z_j)$, and $\mathrm{Gal}(K(z_j)|K)$ can be identified with a subgroup of $\mathfrak{S}_3$ ($1 \leq j \leq r_n$). Therefore $\mathrm{Gal}(L|K)$, which is naturally embedded in the direct product of these $\mathrm{Gal}(K(z_j)|K)$, can be viewed as a subgroup of $\mathfrak{S}_3^{r_n}$. The result then follows from Proposition 1.

Moreover, since every $\mathrm{Gal}(K(z_i)|K))$ is isomorphic to $\mathfrak{S}_3$ or to one of its subgroups of order 2, then, for $1 \leq i, j \leq r_n$, $K(z_i) \cap K(z_j)$ is equal to K or to

$K(z_i)$ or to its quadratic subfield over K. Hence, enumerating the subgroups of $\mathfrak{S}_3$ and the corresponding subfields of $K(z_i)$, we get

LEMMA 5. *For odd $n \geq 9$ and $1 \leq i, j \leq r_n$, $K(z_i) \cap K(z_j)$ is either equal to K or to $K(z_i) = K(z_j)$ or to $K(\sqrt{u_i}) = K(\sqrt{u_j})$, where $u_i = -(4t_i + 3)$.*

Thus, if the degree $[K(\sqrt{u_i}, \sqrt{u_j}) : K] = 2^2$ then $K(z_i) \cap K(z_j) = K$ and $\mathrm{Gal}(K(z_i, z_j)|K) \simeq \mathrm{Gal}(K(z_i)|K) \times \mathrm{Gal}(K(z_j)|K)$. By induction, letting $F = K(\sqrt{u_1}, \ldots, \sqrt{u_{r_n}})$, which is the splitting field of $T_n\left(-\frac{X^2+3}{4}\right)$ over $\mathbb{Q}$, we have:

If $[F : K] = 2^{r_n}$, then $\mathrm{Gal}(L|K)$ is isomorphic to the direct product of the $\mathrm{Gal}(K(z_j)|K)$ $(1 \leq j \leq r_n)$.

The latter holds for the examples we examined ($n \leq 25$). Other computations (for $n \leq 49$) gave $\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathfrak{S}_{r_n}$. These results suggest that, for odd $n \geq 9$, $\mathrm{Gal}(L|Q)$ is plausibly the semi-direct product of $\mathfrak{S}_3^{r_n}$ by $\mathfrak{S}_{r_n}$, or more precisely the wreath product of $\mathfrak{S}_3$ by $\mathfrak{S}_{r_n}$.

In the case where n is a prime number, we also have

PROPOSITION 2. *For prime $n \geq 11$ and any root z of E_n in $\mathbb{C}$, g_z is irreducible over $\mathbb{Q}(t_z)$ and $\mathrm{Gal}(K(z)|K) \simeq \mathrm{Gal}(\mathbb{Q}(z)|\mathbb{Q}(t_z)) \simeq \mathfrak{S}_3$. An irreducible factor of E_n over $\mathbb{Q}$ is a product of some g_z. And E_n is irreducible over $\mathbb{Q}$ if and only if T_n is.*

PROOF. The roots of E_n are algebraic integers (§1). By Lemma 4, if, for some root z of E_n, the degree of u_z is 2, then the minimal polynomial over $\mathbb{Q}$ of a $z_j = e^{i\theta_j}$ in the orbit of z has all its roots of absolute value 1. Hence, by Kronecker's theorem, z_j is a root of unity ([8]), which is impossible (§1). Thus u_z has degree 6, i.e. $u_z = g_z$ and $\mathcal{T}_z = \mathcal{T}$.

4. Factorization modulo a prime.

LEMMA 6. *Let $f \in \mathbb{Z}[X]$ be a reciprocal polynomial such that there exists z in $\mathbb{C} - \{0, -1\}$ for which $\mathrm{Orb}(z)$ consists of 6 distinct roots of f. Then f is reducible modulo every prime p.*

PROOF. The roots of f in $\mathbb{C}$ can be written in the form α/d where α is an algebraic integer and d a fixed positive integer (common denominator). Let $f = \sum_{k=0}^{n} a_j X^j$ and L its splitting field over $\mathbb{Q}$. Consider $h = \frac{d^n}{a_n} f(\frac{X}{d}) = \sum_{j=0}^{n} b_j X^j$, which is in $\mathbb{Z}[X]$, monic, with roots the numerators α of those of f in the ring $\mathcal{O}_L$ of integers of L. Let p be a prime number, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_L$ above p and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_q = \mathcal{O}_L/\mathfrak{p}$ (finite fields with $\mathbb{F}_p \subset \mathbb{F}_q$). For $a \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_L$, let $\underline{a} = a + p\mathbb{Z}$ in $\mathbb{F}_p$ and $\underline{\alpha} = \alpha + \mathfrak{p}$ in $\mathbb{F}_q$; write $\underline{f} = \sum_{k=0}^{n} \underline{a_j} X^j$. Then $\underline{f}$ and $\underline{h}$ are in $\mathbb{F}_p[X]$, and they split in $\mathbb{F}_q[X]$. The degree of $\underline{h}$ is $n \geq 6$. Let $\gamma = dz$, $\gamma_1 = d/z$, $\gamma_2 = -d(z+1)$, $\gamma_3 = -d/(z+1)$ and $\gamma_4 = -d(z+1)/z$; they lie in $d\,\mathrm{Orb}(z)$ and are roots of h. If $\underline{h}$ were irreducible over $\mathbb{F}_p$, then its roots in $\mathbb{F}_q$ would be distinct and there would exist σ_1, σ_2 in $\mathrm{Gal}(\mathbb{F}_p(\underline{\gamma})|\mathbb{F}_p)$ such that $\sigma_i(\underline{\gamma}) = \underline{\gamma_i}$

$(i = 1, 2)$. But then $\sigma_2\sigma_1(\underline{\gamma}) = \underline{\gamma_3}$ and $\sigma_1\sigma_2(\underline{\gamma}) = \underline{\gamma_4}$ being distinct, $\mathrm{Gal}(\mathbb{F}_p(\underline{\gamma})|\mathbb{F}_p)$ would be non abelian, impossible. Thus, $\underline{h}$ is reducible over $\mathbb{F}_p$. It follows, since $d^n f(X) = a_n h(dX)$, that if p does not divide d then $\underline{f}$ is reducible over $\mathbb{F}_p$. If p divides $a_n = a_0$ (f reciprocal), then X divides $\underline{f}$ which is thus reducible over $\mathbb{F}_p$. Now assume p divides d but not a_n. We have $a_n h(\alpha) = \sum_{j=0}^{n} a_j d^{n-j}\alpha^j = 0$. Let $v_\mathfrak{p}$ be the valuation of L at $\mathfrak{p}$. If $v_\mathfrak{p}(\alpha) < v_\mathfrak{p}(d)$ then $v_\mathfrak{p}(a_n\alpha^n) < v_\mathfrak{p}(a_j d^{n-j}\alpha^j)$ for $0 \le j \le n-1$ so that $v_\mathfrak{p}(a_n h(\alpha)) = v_\mathfrak{p}(a_n\alpha^n)$, contradicting $a_n h(\alpha) = 0$. Thus, $v_\mathfrak{p}(\alpha) \ge v_\mathfrak{p}(d)$, for any root α/d of f and any prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ above p. Hence $p^{v_\mathfrak{p}(d)}$ divides all such α and we may remove this factor from d and the α's, thus getting back to the case p does not divide d. Hence $\underline{f}$ is reducible over $\mathbb{F}_p$.

COROLLARY. *For odd $n \ge 9$ and any prime number p, E_n is reducible modulo p.*

PROPOSITION 3. *Let n be a prime ≥ 11. If, for some prime p, $\underline{E_n}$ has at most 3 irreducible factors in $\mathbb{F}_p[X]$, then E_n is irreducible in $\mathbb{Q}[X]$.*

PROOF. Assume E_n is reducible over $\mathbb{Q}$. By Gauss Lemma ([1]), $E_n = FG$ with non-constant $F, G \in \mathbb{Z}[X]$. By Proposition 2, F and G are, to within constant factors, products of some g_z. So there is $z \in \mathbb{C} - \{0, -1\}$ such that $\mathrm{Orb}(z)$ consists of 6 distinct roots of F (resp. G). Also, F and G are reciprocal polynomials. Hence, by Lemma 6, for any prime p, $\underline{F}$ and $\underline{G}$ are products of 2 non-constant polynomials, so that $\underline{E_n}$ has 4 non-trivial factors, in $\mathbb{F}_p[X]$.

5. The case $n = 2p$. Let p be an odd prime number, $\mathbb{Q}_p$ the field of p-adic numbers and v_p the normalized valuation of $\mathbb{Q}_p$. The Newton polygon (e.g. [1]) of a polynomial $f(X) = \sum_{i=0}^{m} a_i X^i$ over $\mathbb{Q}_p$ is the lower convex envelope, in $\mathbb{R}^2$, of the points $(i, v_p(a_i))$ $(0 \le i \le m)$. Let $(x_0, y_0), (x_1, y_1), \ldots, (x_k, y_k)$ be the consecutive vertices of this polygon. Then there are $f_1, \ldots, f_k$ in $\mathbb{Q}_p[X]$ such that $f = \prod_{i=1}^{k} f_i$, the degree of f_i is $x_i - x_{i-1}$ and the roots of f_i, in the splitting field $\hat{L}$ of f over $\mathbb{Q}_p$, have their (normalized) valuation equal to $-e(\hat{L})\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$, where $e(\hat{L})$ is the ramification index of $\hat{L}|\mathbb{Q}_p$, and $\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$ is the slope of the corresponding side of the Newton polygon. Hence, if a natural number d divides the denominator of the reduced fraction $\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$, then for any root γ of f_i in $\hat{L}$, d divides the ramification index of $\mathbb{Q}_p(\gamma)|\mathbb{Q}_p$, so that d divides the degree of any irreducible factor of f_i in $\mathbb{Q}_p[X]$.

We have $E_{2p}(X) = \sum_{k=1}^{2p-1} \binom{2p}{k} X^{k-1}$ and $v_p(\binom{2p}{k}) = 1$ if $k \ne p$, $1 \le k \le 2p-1$ while $v_p(\binom{2p}{p}) = 0$. Therefore the Newton polygon of E_{2p} consists of 2 line segments with vertices $(0, 1), (p-1, 0), (2p-2, 1)$ and slopes $\mp\frac{1}{p-1}$. Hence $E_{2p} = f_1 f_2$, where $f_1, f_2 \in \mathbb{Q}_p[X]$ have degree $p-1$ and are irreducible. It follows that, in $\mathbb{Q}[X]$, E_{2p} is either the product of 2 irreducible factors of degree $p-1$ or is irreducible. Assume that the first case occurs, i.e. $E_{2p} = gh$, with $g, h \in \mathbb{Z}[X]$ irreducible over $\mathbb{Q}$ of degree $p-1$. Then g, h are, like E_{2p}, primitive polynomials i.e. the gcd of their coefficients is 1 (Gauss Lemma). Let $E_{2p}(X) = \sum_{i=0}^{2p-2} a_i X^i$,

$g(X) = \sum_{j=0}^{p-1} b_j X^j$ and $h(X) = \sum_{k=0}^{p-1} c_k X^k$, where the $a_i, b_j, c_k \in \mathbb{Z}$. Since $v_p(a_i) = 1$ for $i \neq p-1$ while $v_p(a_{p-1}) = 0$ and $a_i = \sum_{j+k=i} b_j c_k$ $(0 \leq i \leq 2p-2)$, then, as in the Eisenstein irreducibility criterion ([1]), one of the polynomials g or h, say g, has its constant coefficient b_0 not divisible by p and all its other coefficients b_j $(1 \leq j \leq p-1)$ divisible by p. Let z be a root of g in $\mathbb{C}$. Then $1/z$ is a root of E_{2p} hence of g or h. But $1/z$ is a root of $g_1(X) = X^{p-1}g(\frac{1}{X}) = \sum_{j=0}^{p-1} b_{p-1-j}X^j$, which is an irreducible primitive polynomial of degree $p-1$. If $1/z$ were a root of g and g_1, the two polynomials would be associates in $\mathbb{Q}[X]$ and (since they are primitive) in $\mathbb{Z}[X]$; then $b_{p-1} = \pm b_0$, contradicting the divisibility of the b_j by p. Thus $1/z$ is a root of h and of g_1, which are then associates in $\mathbb{Z}[X]$. Hence $h = \pm g_1$ and $P_{2p}(X) = XE_{2p}(X) = \pm X^p g(X) g(\frac{1}{X})$. Substituting 1 for X, we get $2^{2p} - 2 = \pm g(1)^2$, with $g(1) \in \mathbb{Z}$. This implies that 2 is a quadratic residue modulo 4, a contradiction. Hence

PROPOSITION 4. *For any odd prime p, E_{2p} is irreducible over $\mathbb{Q}$.*

REFERENCES

1. J.W.S. Cassels, *Local Fields.* Cambridge University Press, 1986
2. A. L. Cauchy, *Rapport sur un Mémoire de M. Lamé, relatif au dernier théorème de Fermat.* C. R. Acad. Sci. Paris, 9(1839) 359–363.
3. A. L. Cauchy, *Note sur Quelques Théorèmes d'Algèbre.* in: Exerc. d'Analyse et de Phys. Math. 2 Bachelier, Paris 1841, 137–144 .
4. D. Mirimanoff, *Sur l'équation* $(x+1)^l - x^l - 1 = 0$. Nouv. Ann. Math. 3 (1903) 385–397.
5. P. Morton, *On certain algebraic curves related to polynomial maps.* Compositio Math. 103 (1996) 319–350.
6. P. Ribenboim, *13 Lectures on Fermat's Last Theorem.* Springer Verlag, 1979.
7. G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes.* Acta Arith. 54 (1989) 87–125.
8. L. Washington *Introduction to Cyclotomic Fields.* Springer Verlag, 1982

Pennsylvania State University
25 Yearsley Mill Road
Media, PA 19063
e-mail: cxh22@psu.edu

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (2), 1997 pp. 58–63

BEST UNIFORM RESTRICTED RANGES APPROXIMATION OF COMPLEX-VALUED FUNCTIONS

GEORGEY S. SMIRNOV AND ROMAN G. SMIRNOV

Presented by Vlastimil Dlab, F. R. S. C.

ABSTRACT. We study the uniform best restricted range approximations of complex-valued functions by generalized polynomials. The theory, generalizing the real-valued case, embraces the theorems of existence, characterization, uniqueness and strong uniqueness.

RÉSUMÉ. Nous étudions les meilleur approximations avec image restreint des fonctions de valeures-complexes par polynôms généralisés. Le théorie, en généralisant le cas de valeur réel, comprend les théoèmes de l'existence, unicité at unisité forte.

1. Introduction. The problems of best uniform restricted range approximation have been thoroughly studied in the framework of the well-established theory of best constrained approximation of functions (see the corresponding review in [1] and the relevant references herein, a modern approach to the problem can be found in [2]).

In this article we consider the problem of best uniform restrictied range approximation of *complex valued* continuous functions, which in analogy with the real-valued case [3], can be formulated as follows. *Let $C(Q)$ be a space of complex-valued functions defined on a compact set Q, $P \subset C(Q)$—a finite-dimensional subspace in it and $\Omega = \{\Omega_t \mid t \in Q\}$—a system of non-empty convex and closed sets in $\mathbb{C}$. For a given function $f \in C(Q)$ set:*

$$E(f) := \inf_{p \in P_\Omega} \|f - p\|, \tag{1.1}$$

where

$$P_\Omega = \{p \in P \mid p(t) \in \Omega_t \quad \text{for all} \quad t \in Q\}.$$

Here $\|\ \|$ stands for the uniform norm.

The problem is to investigate the properties of the element $p^* \in P_\Omega$ providing the infimum *in* (1.1).

In this work the problem of existence, characterization, uniqueness and strong uniqueness of such the element p^* is studied for some special system of restrictions

Received by the editors June 1, 1997.
AMS subject classification: 41A10, 41A52.

Ω, using the notion of a *minimal admissible pair of sets* corresponding to the notion of a characteristical set of best approximation in the classical theory of uniform approximation.

2. **Basic definitions, notations and facts.** Let Q be a compact set in the complex plane $\mathbb{C}$ containing at least $n+1$ points. Denote by $C(Q)$ the Banach algebra of all complex-valued continuous functions defined on Q with the norm $\|f\| = \max_{t\in Q} |f(t)|$. For every function $f \in C(Q)$ introduce the set $M(f) := \{t \in Q \mid |f(t)| = \|f\|\}$. Clearly, $M(f)$ is compact. Consider a n-dimensional subspace P with a basis $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$. The elements $p \in P$ have the form $p = \sum_{\nu=1}^{n} c_\nu \varphi_\nu$, where $c_\nu \in \mathbb{C}; \nu = 1, \dots, n$. We call them *generalized polynomials with respect to the system* $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$, or just *polynomials*, for short. For $p \in P$ set $Z(p) := \{t \in Q | p(t) = 0\}$.

DEFINITION 2.1 (4). A subset $P \subset C(Q)$ is called a *Haar space* if every polynomial $p \in P \setminus \{0\}$ has no more than $n-1$ zeros in Q.

Let $u \in C(Q)$ and $r \in C(Q)$ be fixed functions, in addition assume that $r(t) > 0$ for all $t \in Q$. For every point $t \in Q$ denote by Ω_t, $\text{int}\Omega_t$ and $\partial\Omega_t$ correspondingly the closed disk, open disk and circle with the origin $u(t)$ and radius $r(t)$ in $\mathbb{C}$.

HYPOTHESIS 2.1. Throughout this paper we assume that always for some $p_0 \in P$ the condition holds:

$$p_0(t) \in \text{int}\,\Omega_t$$

for all $t \in Q$.

For all $p \in P$ set $B(p) := \{t \in Q \mid p(t) \in \partial\Omega_t\}$. In view of continuity of the functions u, r and p the set $B(p)$ is compact. Introduce the following notation:

$$P_{B,\Omega} := \{p \in P \mid p(t) \in \Omega_t \quad \text{for all} \quad t \in B\},$$

where $B \subset Q$; $P_{\emptyset,\Omega} := P, P_{Q,\Omega} = P_\Omega$. Note that for every set $B \subset Q$ the set $P_{B,\Omega}$ is convex, while for a closed set B $P_{B,\Omega}$ is closed in P. The inclusion $B' \subset B$ obviously implies $P_{B,\Omega} \subset P_{B',\Omega}$.

Let $\mathfrak{M}$ be a set of ordered pairs $(A; B)$, where $A \subset Q, B \subset Q$ and $A \neq \emptyset$. We write $(A'; B') \subset (A; B)$ iff $A' \subset A$ and $B' \subset B$. Then the inclusion $(A'; B') \subset (A; B)$ is called *strict*, if at least one of the inclusions $A' \subset A$ and $B' \subset B$ is strict.

For a function $f \in C(Q)$ and a pair $(A; B) \in \mathfrak{M}$ set

$$E_A(f; P_{B,\Omega}) := \inf_{p\in P_{B,\Omega}} \sup_{t\in A} |f(t) - p(t)|.$$

Clearly, if $A = B = Q$, $E_Q(f; P_{Q,\Omega}) = E_Q(f; P_\Omega) = E(f)$. It is easily seen that the inclusion $(A'; B') \subset (A; B)$ implies the inequality $E_{A'}(f; P_{B',\Omega}) \leq E_A(f; P_{B,\Omega})$, which leads, in particular, to $E_A(f; P_{B,\Omega}) \leq E(f)$ for any pair $(A; B) \in \mathfrak{M}$.

DEFINITION 2.2. A polynomial $q \in P_{B,\Omega}$, satisfying the equality

$$\sup_{t \in A} |f(t) - q(t)| = E_A(f; P_{B,\Omega})$$

is called a *best restricted ranges approximation to f on A from $P_{B,\Omega}$*.

A best restricted ranges approximation to f on Q from P_Ω, or the polynomial $p^* \in P_\Omega$ satisfying

$$\|f - p^*\| = E(f)$$

is called for short a *best approximation to f from P_Ω*.

The compactness argument justifies the validity of the following

THEOREM 2.1. *If A and B are compact subsets of Q ($A \neq \emptyset$), then for every function $f \in C(Q)$ there exists a best restrict ranges approximation to f on A from $P_{B,\Omega}$.*

COROLLARY 2.1. *For every function $f \in C(Q)$ there exists a best approximation to f from P_Ω.*

3. Minimal admissible pairs of sets and their properties. Let $f \in C(Q)$.

DEFINITION 3.1. An ordered pair $(A; B) \in \mathfrak{M}$ is called an *admissible pair (a. p.) for a function f with respect to P_Ω*, if

$$E_A(f; P_{B,\Omega}) = E(f).$$

DEFINITION 3.2. An admissible pair $(A_0; B_0)$ for f with respect to P_Ω is called a *minimal admissible pair (m. a. p.) for a function f* with respect to P_Ω, if the *strict* inclusion $(A; B) \subset (A_0; B_0)$ implies the absolute inequality:

$$E_A(f; P_{B,\Omega}) < E_{A_0}(f; P_{B_0,\Omega}).$$

REMARK 3.1. *Each a. p. $(A; B)$ for a function f, where A and B are finite subsets of Q, admits at least one m. a. p. for f.*

THEOREM 3.1. *Let $(A_0; B_0) \in \mathfrak{M}$ be a m. a. p. for $f \in C(Q)$ with respect to P_Ω, and $p^* \in P_\Omega$ is a best approximation to f from P_Ω. Then simultaneously the following inclusions hold:*

$$A_0 \subset M(f - p^*), \qquad B_0 \subset B(p^*). \tag{3.2}$$

THEOREM 3.2. *For each function $f \in C(Q)$ there exists at least one m. a. p. $(A_0; B_0)$ for f with respect to P_Ω, such that $|A_0 \cup B_0| \leq 2n + 1$.*

DEFINITION 3.3. We call a function $f \in C(Q)$ *admissible*, if it satisfies at least one of the two conditions:

1. $f(t) \in \Omega_t$ for all $t \in Q$;
2. $M(f - p^*) \cap B(p^*) = \emptyset$,

where $p^* \in P_\Omega$ is some best approximation to f from P_Ω.

We denote the set of all admissible functions by $C_a(Q)$.

THEOREM 3.3. *Let P be a Haar space and $f \in C_a(Q) \setminus P_\Omega$. Then each m. a. p. $(A_0; B_0)$ for the function f with respect to P_Ω satisfies the condition $|A_0 \cup B_0| \geq n + 1$.*

4. **Characterization of best approximation.** Let $f \in C(Q)$, $p^* \in P_\Omega$. Set $\sigma_1(t) := f(t) - p^*(t)$, $t \in M(f - p^*)$, and $\sigma_2(t) := u(t) - p^*(t)$, $t \in B(p^*)$.

THEOREM 4.1 (KOLMOGOROV-TYPE CHARACTERIZATION). *A polynomial $p^* \in P_\Omega$ is a best approximation to a function $f \in C(Q)$ from P_Ω, if and only if for each $p \in P$ the conditional inequality holds true*

$$\min\left\{ \min_{t \in M(f-p^*)} \operatorname{Re}(p(t)\overline{\sigma_1(t)}), \min_{t \in B(p^*)} \operatorname{Re}(p(t)\overline{\sigma_2(t)}) \right\} \leq 0 \tag{4.3}$$

For each function $f \in C(Q)$ and $p^* \in P_\Omega$ consider the set

$$\begin{aligned} \mathcal{B} = \{\mathbf{b}(t) &= (\overline{\phi_1(t)}, \overline{\phi_2(t)}, \ldots, \overline{\phi_n(t)})\sigma_1(t),\ t \in M(f - p^*)\} \\ &\cup \{\mathbf{c}(t) = (\overline{\phi_1(t)}, \overline{\phi_2(t)}, \ldots, \overline{\phi_n(t)})\sigma_2(t),\ t \in B(p^*)\}, \end{aligned}$$

noticing that due to compactness of the sets $M(f - p^*)$ and $B(p^*)$ the set B is compact in $\mathbb{C}^n$.

THEOREM 4.2 ("ZERO IN THE CONVEX HULL" CHARACTERIZATION). *A polynomial $p^* \in P_\Omega$ is a best approximation to a function $f \in C(Q) \setminus P_\Omega$ if and only if the origin of the space $\mathbb{C}^n$ belongs to the convex hull of $\mathcal{B}$.*

THEOREM 4.3. *A polynomial $p^* \in P_\Omega$ is a best approximation to $f \in C(Q) \setminus P_\Omega$ from P_Ω if and only if there exist such sets $A_0 = \{t_1, t_2, \ldots t_k\} \subset M(f - p^*)$, $B_0 = \{t'_1, t'_2, \ldots, t'_m\} \subset B(p^*)$ $(k \geq 1, k + m \leq 2n + 1)$ and positive constants $\lambda_1, \ldots, \lambda_k$, $\lambda'_1, \ldots, \lambda'_m$, that for each polynomial $p \in P$ the condition holds:*

$$\sum_{l=1}^{k} \lambda_l p(t_l)\overline{\sigma_1(t_l)} + \sum_{s=1}^{m} \lambda'_s p(t'_s)\overline{\sigma_2(t'_s)} = 0 \tag{4.4}$$

REMARK 4.1. *Under the conditions of Theorem 4.3*

$$|A_0 \cup B_0| \leq 2n + 1 - |A_0 \cap B_0|.$$

REMARK 4.2. *If P is a Haar space and $f \in C_a(Q) \setminus P_\Omega$, the sets A_0 and B_0 in Theorem 4.3 additionally satisfy the condition $|A_0 \cup B_0| \geq n + 1$.*

5. Uniqueness and strong uniqueness of best approximation. We assume throughout this section that P is a Haar space.

THEOREM 5.1 (UNIQUENESS THEOREM). *Each function $f \in C_a(Q)$ has a unique best approximation in P_Ω.*

THEOREM 5.2 (STRONG UNIQUENESS THEOREM). *Let $p^* \in P_\Omega$ be a best approximation to a function $f \in C_a(Q)$ from P_Ω. Then there exists such a constant $\gamma = \gamma(f) > 0$ that any polynomial $p \in P_\Omega$ satisfies the inequality:*

$$\|f - p\|^2 \geq \|f - p^*\|^2 + \gamma\|p^* - p\|^2. \tag{5.5}$$

Define on the set $C_a(Q)$ the *operator of best approximation* τ, which assigns to each function $f \in C_a(Q)$ its unique best approximation in P_Ω.

THEOREM 5.3. *The operator τ is continuous in $C_a(Q)$.*

REMARK 5.1. Theorem 5.2 suggests the standard form of the inequality of strong uniqueness (see [5]) in the complex case. Indeed, set $\gamma_1 = 1/4\gamma, \delta = 2\gamma^{-1/2}$. Then for all such $p \in P_\Omega$ that $\|p - p^*\| \leq \delta$ we have the following inequality

$$\|f - p\| \geq \|f - p^*\| + \gamma_1\|p - p^*\|^2.$$

6. Conclusion. All the results of this paper remain valid for some weakened system of restrictions Ω_t, which can be defined as follows. Let X is some open subset of Q, then

$$\Omega_t := \begin{cases} \{z \in \mathbb{C} \mid |z - u(t)| \leq r(t)\} & \text{for } t \in Q \setminus X \\ \mathbb{C} & \text{for } t \in X; \end{cases}$$

moreover, the functions u and r are continuous on $Q \setminus X$ and in addition, the function r is positive on $Q \setminus X$.

A full version of this article containing all the proofs and elucidating details will be published elsewhere [6].

ACKNOWLEDGMENTS. The authors acknowledge stimulating discussions on the subject of this work with Vladislav Dzyadyk, Victor Konovalov and Igor Shevchuk, as well as a technical help from Terrilynn Ho and Jamie Mingo in preparation of the manuscript.

The research was supported in part by the National Science and Engineering Research Council of Canada.

REFERENCES

1. B. L. Chalmers and G. D. Taylor, *Uniform approximation with constraints.* Jahresber. Deutsch. Math.-Verein. **81** (1978/1979), 49–86.
2. A. Kroó and D. Schmidt, *A Haar-type theory of best uniform approximation with constraints* Acta Math. Hungar. **58** (1991), no. 3-4, 351–374.
3. G. D. Taylor, *On approximation by polynomials having restricted ranges.* SIAM. J. Numer. Anal. **5** (1968), 258–268.
4. R. A. DeVore and G. G. Lorentz, *Constructive Approximation.* Springer-Verlag, New York, 1993.
5. D. J. Newman and H. S. Shapiro, *Some theorems on Chebyshev approximation.* Duke Math. J. **30** (1963), 673–682.
6. G. S. Smirnov and R. G. Smirnov, *Best uniform approximation of complex valued functions by generalized polynomials having restricted ranges.* Preprint, Queen's University, 1997.

Department of Mechanics and Mathematics
Kyiv National University
6 Glushkova Ave.
Kyiv, UKRAINE, 252127.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, CANADA, K7L 3N6
e-mail: smirnovr@mast.queensu.ca.

C. R. Math. Rep. Acad. Sci. Canada Vol. **19** (2), 1997 p. 64

CORRIGENDUM TO FALTINGS PLUS EPSILON, WILES PLUS EPSILON, AND THE GENERALIZED FERMAT EQUATION

H. DARMON

On page 7, line -11: after "differently:": remove the rest of the paragraph, and replace it by: "the stalk $\mathcal{O}_{\underline{X},P}$ for this sheaf is defined to be the ring of Puiseux series in t_P^{1/m_P}." That should end the paragraph.

Received by the editors November 6, 1997.