BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 25, Number 1, July 1991

ELLIPTIC CURVES AND REAL ALGEBRAIC MORPHISMS INTO THE 2-SPHERE

J. BOCHNAK AND W. KUCHARZ

Given affine nonsingular real algebraic varieties X and Y, let $\mathscr{R}(X, Y)$ denote the set of regular mappings, that is, real algebraic morphisms, form X into Y. (By affine real algebraic variety we mean, up to isomorphism, an algebraic subset of $\mathbf{R}^n$ equipped with the sheaf of $\mathbf{R}$-valued regular functions [1, Definition 3.2.9]. Recall that projective real algebraic varieties are actually affine [1, Theorem 3.4.4].) We consider $\mathscr{R}(X, Y)$ as a subset of the space $C^\infty(X, Y)$ of C^∞ mappings from X into Y endowed with C^∞ topology. We also assume that X is compact. The classical theorem of Stone-Weierstrass implies that $\mathscr{R}(X, Y)$ is dense in $C^\infty(X, Y)$ if $Y = \mathbf{R}^k$. Here we try to extend this result to $Y = S^2$, the unit sphere in $\mathbf{R}^3$. This problem is already difficult (cf. [1, 3, 4]) and leads, as we show below, to interesting relations between real regular mappings and arithmetical properties of real algebraic varieties.

Given f in $C^\infty(X, Y)$, consider the following two conditions:

(i) f belongs to the closure of $\mathscr{R}(X, Y)$ in $C^\infty(X, Y)$,

(ii) f is homotopic to a regular mapping.

In general, neither (i) nor (ii) is satisfied, even for $Y = S^k$, the unit sphere in $\mathbf{R}^{k+1}$ (cf. [1, 3, 4]). Clearly (i) implies (ii), while the converse is not always true. It is remarkable that (ii) does imply (i) for $Y = S^k$ with $k = 1, 2$, or 4 [1, Theorem 13.3.4] (for further results on (i) and (ii) the reader may consult [1, 2, 3, 4, 6, 7]).

Since (i) and (ii) are equivalent for $Y = S^2$, it follows that for each affine nonsingular real algebraic surface X, which is compact, connected, and oriented, there exists a uniquely determined nonnegative integer $b(X)$ such that the closure of $\mathscr{R}(X, S^2)$ in

Received by the editors July 18, 1990 and, in revised form, December 3, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14G30, 14C99, 57R19.
The second author was supported by NSF Grant DMS-8905538.

$C^\infty(X, S^2)$ is equal to

$$\{f \in C^\infty(X, S^2) | \deg(f) \text{ is a multiple of } b(X)\}.$$

The above statement holds since the topological degree $\deg: \pi^2(X) \to \mathbf{Z}$ is an isomorphism from the second cohomotopy group $\pi^2(X)$ of X onto $\mathbf{Z}$ and, by [1, Proposition 13.4.2], the set $\pi^2_{\text{alg}}(X) = \{[f] \in \pi^2(X) | f \in \mathscr{R}(X, S^2)\}$ is a subgroup of $\pi^2(X)$. The invariant $b(X)$ can attain, as X varies, any nonnegative integer value (this answers a question raised in [1, Remark 13.4.3]). More precisely, we have the following.

Theorem 1. *Let M be a C^∞ compact connected oriented surface and let b be a nonnegative integer. Then there exists an affine nonsingular real algebraic surface X, diffeomorphic to M, such that $b(X) = b$.*

One of the essential steps in the proof of Theorem 1 is the study of $\mathscr{R}(C \times D, S^2)$, where C and D are nonsingular real cubic curves in $\mathbf{R}P^2$. This study, influenced by arithmetical properties of elliptic curves, deserves special attention.

Given $\alpha \in \mathbf{R}^\star = \mathbf{R}\backslash\{0\}$, let $\tau_\alpha = (1/2)(1 + \alpha\sqrt{-1})$ if $\alpha > 0$, and $\tau_\alpha = \alpha\sqrt{-1}$ if $\alpha < 0$ and set

$$D_\alpha = \{[x: y: z] \in \mathbf{R}P^2 | y^2 z = 4x^3 - g_2(\tau_\alpha)xz^2 - g_3(\tau_\alpha)z^3\},$$

where, as usual, the $g_j(\tau_\alpha)$ are the numbers (in this case real) defined by

$$g_2(\tau_\alpha) = 60 \sum_{\omega \in \Lambda'_\alpha} \omega^{-4}, \qquad g_3(\tau_\alpha) = 140 \sum_{\omega \in \Lambda'_\alpha} \omega^{-6},$$

$\Lambda_\alpha = \mathbf{Z} + \mathbf{Z}\tau_\alpha$ is a lattice in $\mathbf{C}$, $\Lambda'_\alpha = \Lambda_\alpha \backslash \{0\}$ (cf. [5]). Each D_α is then a nonsingular real cubic curve in $\mathbf{R}P^2$, connected if $\alpha > 0$, and having 2 connected components if $\alpha < 0$. Moreover, D_α and D_β are not biregularly isomorphic for $\alpha \neq \beta$, and every nonsingular real cubic curve in $\mathbf{R}P^2$ is isomorphic (through a linear isomorphism of $\mathbf{R}P^2$) to some D_α. It follows that $\mathbf{R}^\star$ can be regarded as a moduli space for nonsingular real cubic curves in $\mathbf{R}P^2$.

Proposition 2. *Let C and D be nonsingular real cubic curves in $\mathbf{R}P^2$. Then $C \times D$ can be oriented in such a way that for each f in $\mathscr{R}(C \times D, S^2)$, the topological degree $\deg(f|A)$ of the restriction* *of f to a connected component A of $C \times D$ does not depend on the choice of A. Moreover, the set*

$$\mathrm{Deg}_{\mathscr{R}}(C, D) = \{m \in \mathbf{Z} | m = \deg(f|A), f \in \mathscr{R}(C \times D, S^2)\}$$

is a subgroup of $\mathbf{Z}$.

One can show that if $C \times D$ is replaced by a compact oriented affine nonsingular irreducible surface X, then, in general $|\deg(f|A)|$ depends on the choice of the connected component A of X for f in $\mathscr{R}(X, S^2)$.

Since (i) and (ii) are equivalent for $Y = S^2$, it follows that the unique nonnegative integer $b(C, D)$ satisfying $\mathrm{Deg}_{\mathscr{R}}(C, D) = b(C, D)\mathbf{Z}$ (obviously, $b(C, D) = b(C \times D)$ if both C and D are connected) fully determines the closure of $\mathscr{R}(C \times D, S^2)$ in $C^\infty(C \times D, S^2)$: a C^∞ mapping $f: C \times D \to S^2$ belongs to the closure of $\mathscr{R}(C \times D, S^2)$ in $C^\infty(C \times D, S^2)$ if and only if for every connected component A of $C \times D$, one has $\deg(f|A) = b(C, D)p$ for some integer p independent of A. In particular, $\mathscr{R}(C \times D, S^2)$ is dense in $C^\infty(C \times D, S^2)$ if and only if $C \times D$ is connected and $b(C, D) = 1$. Also, $\mathscr{R}(C \times D, S^2)$ consists of the null homotopic regular mappings if and only if $b(C, D) = 0$.

It turns out that the invariant $b(D_\alpha, D_\beta)$ can be explicitly computed as a function of $(\alpha, \beta) \in \mathbf{R}^\star \times \mathbf{R}^\star$, which clarifies then completely the structure of the closure of $\mathscr{R}(C \times D, S^2)$ in $C^\infty(C \times D, S^2)$ for the product of arbitrary nonsingular real cubic curves C and D in $\mathbf{R}P^2$.

Theorem 3. *Let α and β be in $\mathbf{R}^\star$. Then $b(D_\alpha, D_\beta) = 0$ if and only if the product $\alpha\beta$ is in $\mathbf{R} \backslash \mathbf{Q}$.*

In particular, $b(D_\alpha, D_\alpha) \neq 0$ if and only if $\alpha^2 \in \mathbf{Q}$ (that is, if the complexification $D_{\alpha\mathbf{C}} \subset \mathbf{C}P^2$ of D_α is an elliptic curve with complex multiplication).

Let us now consider the case where $\alpha\beta$ is in $\mathbf{Q}$. Let $\mathbf{Z}^+$ denote the set of strictly positive integers. Given integers p and q, let (p, q) denote their greatest common divisor.

Theorem 4. *Let $\alpha, \beta \in \mathbf{R}^\star$, $\alpha > 0$, $\beta > 0$ (that is, D_α and D_β are connected real cubic curves) and $\alpha\beta \in \mathbf{Q}$.*

I. *Assume $\alpha^2 \notin \mathbf{Q}$ and let $\alpha\beta = 4p/q$, where $p, q \in \mathbf{Z}^+$, $(p, q) = 1$, $q = 2^k r$, $k \geq 0$, $r \in \mathbf{Z}^+$, $r \equiv 1 \pmod 2$.*

Then

$$b(D_\alpha, D_\beta) = \begin{cases} 4q & \text{if } k = 0, \\ 2q & \text{if } k = 1, \\ q/2 & \text{if } k = 2, \\ q & \text{if } k \geq 3. \end{cases}$$

II. *Assume* $\alpha^2 \in \mathbf{Q}$ *and let* $\alpha = (p_1/r_1)\sqrt{d}$, $\beta = (p_2/r_2)\sqrt{d}$, *where* p_j, r_j, $d \in \mathbf{Z}^+$, $(p_j, r_j) = 1$, $p_j = 2^{l_j} m_j$, $r_j = 2^{s_j} n_j$, $l_j \geq 0$, $s_j \geq 0$, m_j, $n_j \in \mathbf{Z}^+$, $m_j n_j \equiv 1 \pmod 2$ *for* $j = 1, 2$, *and* d *is square free. Define*

$$\xi = \frac{r_1 r_2}{(p_1 p_2 d, r_1 r_2)}.$$

Then

$$b(D_\alpha, D_\beta) = \begin{cases} \xi & \text{if } l_1 = l_2 = s_1 = s_2 = 0 \text{ and } d \equiv 3 \pmod 4, \\ 4\xi & \text{if } l_1 = l_2 = s_1 = s_2 = 0 \text{ and } d \equiv 2 \pmod 4, \\ & \text{or } l_1 = l_2 > 0, \text{ or } s_1 = s_2 > 0, \\ 2\xi & \text{in all other cases.} \end{cases}$$

For the lack of space we do not give here formulas for $b(D_\alpha, D_\beta)$ with $\alpha \in \mathbf{R}^\star$, $\beta < 0$. Instead we record some interesting corollaries to Proposition 2 and Theorems 3 and 4.

Corollary 5. *Let* C *and* D *be nonsingular real cubic curves in* $\mathbf{R}P^2$. *Then the following conditions are equivalent*:

(a) $\mathscr{R}(C \times D, S^2)$ *is dense in* $C^\infty(C \times D, S^2)$;

(b) (C, D) *is a pair of cubics biregularly isomorphic to* (D_α, D_β), *where* $\alpha = (p_1/r_1)\sqrt{d}$, $\beta = (p_2/r_2)\sqrt{d}$, *with* p_j, r_j, $d \in \mathbf{Z}^+$, $j = 1, 2$, d *square free,* $d \equiv 3 \pmod 4$, $p_1 p_2 r_1 r_2 \equiv 1 \pmod 2$, *and* $p_1 p_2 d$ *divisible by* $r_1 r_2$. □

Corollary 6. *Given a nonnegative integer* b, *there exists a connected nonsingular real cubic curve* C *in* $\mathbf{R}P^2$ *such that* $b(C, C) = b$.

Proof. For $b = 0$, it suffices to take $C = D_\alpha$, where $\alpha > 0$, $\alpha^2 \notin \mathbf{Q}$ (cf. Theorem 3). For $b > 0$, one can take $C = D_\alpha$ with $\alpha = \sqrt{(4 + 3b)/b}$ (cf. Theorem 4). □

Corollary 7. *There exist, up to isomorphism, precisely* 18 *unordered pairs* $\{C, D\}$ *of nonsingular real cubic curves in* $\mathbf{R}P^2$, *defined over* $\mathbf{Q}$, *such that* $\mathscr{R}(C \times D, S^2)$ *is dense in* $C^\infty(C \times D, S^2)$. *More* *precisely, these unordered pairs are* $\{A_k, A_k\}$, $\{A_k, A_k^\star\}$ *for* $k = 1, \dots, 8$, $\{A_1, A_5\}$ *and* $\{A_1^\star, A_5\}$, *where (in affine coordinates)*

$$A_1 : y^2 = x^3 - 1, \qquad A_1^\star : y^2 = x^3 + 1$$
$$A_k : y^2 = 4x^3 - a_k x - a_k, \qquad A_k^\star : y^2 = 4x^3 - a_k x + a_k$$

for $k = 2, \dots, 8$, *with* $a_k = 27j_k/(j_k - 1728)$ *and*

k	2	3	4	5	6
$-j_k$	$(3\cdot 5)^3$	2^{15}	$(2^5\cdot 3)^3$	$2^{15}\cdot 3\cdot 5^3$	$(2^6\cdot 3\cdot 5)^3$

k	7	8
$-j_k$	$(2^5\cdot 3\cdot 5\cdot 11)^3$	$(2^6\cdot 3\cdot 5\cdot 23\cdot 29)^3$

Sketch of proof. Applying [5, p. 233], one can describe explicitly the set Γ of all elements α in $\mathbf{R}^\star$ such that D_α is isomorphic to a real cubic in $\mathbf{R}P^2$, defined over $\mathbf{Q}$, and the complexification $D_{\alpha\mathbf{C}} \subset \mathbf{C}P^2$ of D_α has complex multiplication (that is, $\alpha^2 \in \mathbf{Q}$). The set Γ has 26 elements and one checks, using Corollary 5, that $b(D_\alpha, D_\beta) = 1$ for precisely 18 unordered pairs $\{\alpha, \beta\}$ with $\alpha, \beta \in \Gamma$, $\alpha > 0$, $\beta > 0$. Thus the first part of Corollary 7 follows. Moreover, in the process described above, one obtains explicit equations for the real cubics in $\mathbf{R}P^2$, defined over $\mathbf{Q}$, which correspond to the D_α with α in Γ. This implies the second part of Corollary 7. □

Sketch of proofs of Proposition 2 *and Theorems* 3 *and* 4. Fix α, β in $\mathbf{R}^\star$. Let E_α, $E_\beta \subset \mathbf{C}P^2$ be the complexification of D_α, D_β, respectively. We shall identify, as usual, $\mathrm{Hom}(E_\alpha, E_\beta)$ with

$$H(\alpha, \beta) = \{\lambda = a + b\tau_\beta \in \mathbf{C} | a, b \in \mathbf{Z} \text{ and } \lambda\tau_\alpha = c + d\tau_\beta \text{ for some } c, d \in \mathbf{Z}\}.$$

Denote by $H^2_{\mathrm{alg}}(E_\alpha \times E_\beta, \mathbf{Z})$ the subgroup of $H^2(E_\alpha \times E_\beta, \mathbf{Z})$ which consists of the cohomology classes $[[\Delta]]$ of all divisors Δ on $E_\alpha \times E_\beta$. Since E_α and E_β are complex elliptic curves, the group $H^2_{\mathrm{alg}}(E_\alpha \times E_\beta, \mathbf{Z})$ is generated by $[[\{0\} \times E_\beta]]$ and all elements of the form $[[\text{graph } \lambda]]$ for λ in $H(\alpha, \beta)$. Moreover, choosing an orientation on D_α (resp. D_β) so that if D_α (resp. D_β) has two connected components, then their homology classes in $H_1(E_\alpha, \mathbf{Z})$ (resp. $H_1(E_\beta, \mathbf{Z})$) are equal, one obtains

$$(*)\quad i_A^\star(H^2_{\mathrm{alg}}(E_\alpha \times E_\beta, \mathbf{Z})) = \{b \in \mathbf{Z} | \lambda = a + b\tau_\beta \in H(\alpha, \beta) \text{ for some } a \in \mathbf{Z}\}$$

where A is an arbitrary connected component of $D_\alpha \times D_\beta$, i_A: $A \to E_\alpha \times E_\beta$ is the inclusion mapping, and $H^2(A, \mathbf{Z})$ is identified with $\mathbf{Z}$. This can be seen identifying E_α and E_β with $\mathbf{C}/\Lambda_\alpha$ and $\mathbf{C}/\Lambda_\beta$, respectively.

Let $f\colon D_\alpha \times D_\beta \to S^2$ be a C^∞ mapping and let v be a generator of $H^2(S^2, \mathbf{Z})$. It follows from [3] that f belongs to the closure of $\mathscr{R}(D_\alpha \times D_\beta, S^2)$ in $C^\infty(D_\alpha \times D_\beta, S^2)$ if and only if $f^\star(v)$ is in

$$H^2_{\mathbf{C}-\mathrm{alg}}(D_\alpha \times D_\beta, \mathbf{Z}) = i^\star(H^2_{\mathrm{alg}}(E_\alpha \times E_\beta, \mathbf{Z})),$$

where $i\colon D_\alpha \times D_\beta \to E_\alpha \times E_\beta$ is the inclusion mapping. This, together with $(*)$, implies Proposition 2. In particular, $b(D_\alpha, D_\beta)$ is well defined. It also follows that $b(D_\alpha, D_\beta)$ is equal to the nonnegative integer $b(\alpha, \beta)$ which generates the group in $(*)$. The computation of $b(\alpha, \beta)$ is purely arithmetical and yields Theorems 3 and 4. □

A special case of Theorem 1, with M of topological genus 1, is contained in Corollary 6. This is a starting point for the proof of the general case, which requires several constructions of the type used in [3, 4].

We also have several results concerning $\mathscr{R}(X_1 \times X_2, S^2)$ for real algebraic curves X_1 and X_2 other than cubic curves. For example, let F_n be the Fermat curve in $\mathbf{R}P^2$ given by the equation $x^n + y^n = z^n$. Then one can show that $\mathscr{R}(F_n \times F_n, S^2)$ is dense in $C^\infty(F_n \times F_n, S^2)$ for n odd, $n \geq 3$, and that $\mathscr{R}(F_k \times F_k, S^2)$, with k even, $k \geq 4$, contains mappings which are not null homotopic. Previously, it was only known that every regular mapping from $F_2 \times F_2$ into S^2 is null homotopic [2, 7].

References

1. J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie Algébrique Réelle*, Ergeb. Math. Grenzgeb., vol. 12, Springer-Verlag, Berlin and New York, 1987.
2. J. Bochnak and W. Kucharz, *Representation of homotopy classes by algebraic mappings*, J. Reine Angew. Math. **377** (1987), 159–169.

3. ——, *On real algebraic morphisms into even-dimensional spheres*, Ann. of Math. (2) **128** (1988), 415–433.

4. ——, *Algebraic models of smooth manifolds*, Invent. Math. **97** (1989), 585–611.

5. D. Husemoller, *Elliptic curves*, Springer-Verlag, Berlin and New York, 1987.

6. N. Ivanov, *Approximation of smooth manifolds by real algebraic sets*, Russian Math. Surveys **37** (1982), 1–59.

7. J.-L. Loday, *Applications algébriques du tore dans la sphère et de $S^p \times S^q$ dans S^{p+q}*, Algebraic K-Theory. II, Lecture Notes in Math., vol. 342, Springer-Verlag, Berlin and New York, 1973, pp. 79–91.

DEPARTMENT OF MATHEMATICS, VRIJE UNIVERSITEIT, 1007 MC AMSTERDAM, THE NETHERLANDS

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII AT MANOA, 2565 THE MALL, HONOLULU, HAWAII 96822