COMPOSITIO MATHEMATICA

Corrigendum: '*On certain algebraic curves related to polynomial maps*, Compositio Math. 103 (1996), 319–350'

Patrick Morton

Compositio Math. **147** (2011), 332–334.

doi:10.1112/S0010437X1000480X

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

Compositio Math. 147 (2011) 332–334
doi:10.1112/S0010437X1000480X

Corrigendum: '*On certain algebraic curves related to polynomial maps*, Compositio Math. 103 (1996), 319–350'

Patrick Morton

Abstract

An argument is given to fill a gap in a proof in the author's article *On certain algebraic curves related to polynomial maps*, Compositio Math. **103** (1996), 319–350, that the polynomial $\Phi_n(x, c)$, whose roots are the periodic points of period n of a certain polynomial map $x \to f(x, c)$, is absolutely irreducible over the finite field of p elements, provided that $f(x, 1)$ has distinct roots and that the multipliers of the orbits of period n are also distinct over $\mathbb{F}_p$. Assuming that $\Phi_n(x, c)$ is reducible in characteristic p, we show that Hensel's lemma and Laurent series expansions of the roots can be used to obtain a factorization of $\Phi_n(x, c)$ in characteristic 0, contradicting the absolute irreducibility of this polynomial over the rational field.

In [Mor96, Theorem 15] it is asserted that the nth dynatomic polynomial

$$\Phi_n(x) = \prod_{d|n} (f^d(x) - x)^{\mu(n/d)}$$

(see [Sil07, p. 148]) associated to the dynamical system $x \to f(x) = f(x, c)$ is irreducible over the algebraic closure $\bar{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ if the polynomial $f(x, c) \in \mathbb{Z}[x, c]$ satisfies certain conditions (H) [Mor96, p. 323] and $f(x, 1)$ and $\delta_n(1, c)$ have distinct roots over $\mathbb{F}_p$, where $\delta_n(x, c)$ is the monic polynomial whose roots are the multipliers of the orbits of roots of $\Phi_n(x)$ under the map $f(x)$. (See p. 321; this and all other page references are to [Mor96] unless noted otherwise.)

The argument presented here fills a gap in the proof of this theorem. In Case 2 (p. 346), it was assumed that $\Phi_n(x) = A(x)B(x)$ over the field $\tilde{F}$, which is the splitting field of $f(x, 1)$ over $\mathbb{F}_p$; it was then deduced that $\Phi_n(x) = \tilde{A}(x)\tilde{B}(x)$ over the field $K_p(c)$, where K_p is a finite extension of the p-adic field $\mathbb{Q}_p$ with residue class field $\tilde{F}$. However, from the proof of Hensel's lemma [Has69, p. 161] it only follows that the coefficients in this factorization are elements of the formal power series ring $R[[c]]$, where R is the ring of integers in K_p. It is possible to show that the coefficients are actually in $R[c]$, i.e. that $\tilde{A}(x, c)$ and $\tilde{B}(x, c)$ lie in $R[x, c]$, by the following argument.

If π is a prime element of R, then the proof of Hensel's lemma constructs $\tilde{A}(x) = \tilde{A}(x, c)$ and $\tilde{B}(x) = \tilde{B}(x, c)$ by extending the congruence

$$\Phi_n(x) \equiv A(x)B(x) \pmod{\pi}$$

Received 19 October 2009, accepted in final form 16 February 2010, published online 18 June 2010.
2000 Mathematics Subject Classification 37P05 (primary), 37P25 (secondary).
Keywords: dynatomic polynomial, absolute irreducibility, Hensel's lemma, Laurent series expansions.

to a congruence of the form

$$\Phi_n(x) \equiv A_r(x)B_r(x) \pmod{\pi^r} \quad \text{for } r \geqslant 1,$$

where A_r and B_r are polynomials in $R[x, c]$ with $A_r(x) \equiv A(x)$ and $B_r(x) \equiv B(x) \pmod{\pi}$. Then

$$\tilde{A}(x) = \tilde{A}(x, c) = \lim_{r\to\infty} A_r(x), \quad \tilde{B}(x) = \tilde{B}(x, c) = \lim_{r\to\infty} B_r(x).$$

We now use the series

$$z_s = z(u) = \zeta u + \frac{a_1}{u} + \frac{a_2}{u^2} + \cdots \tag{1}$$

of [Mor96, Lemma 2], defined over the field K_p, where ζ is a root of $f(x, 1) = 0$ and $u^m = c$. It is clear from the proof of [Mor96, Lemma 1] that the coefficients of z_s lie in R and that the different series z_s, when reduced mod π, give all the roots of $\Phi_n(x)$ over $\tilde{F}((1/u)) = R/\pi((1/u))$. Substituting z_s into $\Phi_n(x)$ gives

$$0 \equiv \Phi_n(z_s) \equiv A_r(z_s)B_r(z_s) \pmod{\pi^r},$$

and hence π divides either $A_r(z_s)$ or $B_r(z_s)$. But, by the argument given in Case 2 (p. 346), π cannot divide both of these expressions since $A(x)$ and $B(x)$ have no common roots over $\tilde{F}$. Therefore z_s is a root of A_r or B_r (mod π^r), and it follows that $(x - z_s)$ divides $A_r(x)$ or $B_r(x)$ (mod π^r). Since the different series are distinct mod π, we have

$$A_r(x) \equiv \prod_{s\in I}(x - z_s) \quad \text{and} \quad B_r(x) \equiv \prod_{s'\in J}(x - z_{s'}) \pmod{\pi^r}, \tag{2}$$

where the products are taken over certain sets I and J of sequences of roots of $f(x, 1) = 0$ (see [Mor96, Lemmas 1 and 2]). Now, by (1), the degrees in u of both products in (2) are bounded from above; and because $u^m = c$, this is also true of the degree in c. Using the fact that the coefficients on both sides of the equations in (2) are elements of the Laurent series ring $R/\pi^r((1/u))$, it follows that the coefficients of the polynomials $A_r(x)$ and $B_r(x)$ can be taken to be polynomials in c whose degrees are bounded by some integer N which is independent of r.

This argument gives that

$$A_r(x) = \sum_{i\leqslant d_1, j\leqslant N} a_{ij}^{(r)} x^i c^j \quad \text{and} \quad B_r(x) = \sum_{i\leqslant d_2, j\leqslant N} b_{ij}^{(r)} x^i c^j,$$

where d_1 and d_2 are the degrees in x of $A(x)$ and $B(x)$, respectively, and $a_{ij}^{(r)}, b_{ij}^{(r)} \in R$. From the construction of Hensel's lemma we get that

$$a_{ij}^{(r+1)} \equiv a_{ij}^{(r)} \quad \text{and} \quad b_{ij}^{(r+1)} \equiv b_{ij}^{(r)} \pmod{\pi^r},$$

so for each pair (i, j) the sequences $\{a_{ij}^{(r)}\}$ and $\{b_{ij}^{(r)}\}$ converge in R as $r \to \infty$. Hence $\tilde{A}(x), \tilde{B}(x) \in R[x, c]$, as required. The rest of the proof in Case 2 of [Mor96, Theorem 15] is now valid.

The same arguments can be used to finish the proof of [Mor96, Proposition 17, p. 346].

We also point out that the references to papers [17–20] in the bibliography of [Mor96] should be to the papers [16–19].

Note that [Mor96, Theorem 15] was used in [Mor98] to prove that over an arbitrary field κ, $\Phi_n(x, c)$ is irreducible if: (i) for some $m \geqslant 1$, $f(x, u^m)$ is homogeneous in x and u of degree at least two; (ii) $f(x, 0) = x^k$; (iii) $f(x, 1)$ and $\delta_n(1, c)$ have distinct roots over κ.

Acknowledgement

I am grateful to an anonymous referee for helpful criticism which led me to clarify the above argument.

References

Has69 H. Hasse, *Zahlentheorie* (Akademie Verlag, Berlin, 1969).

Mor96 P. Morton, *On certain algebraic curves related to polynomial maps*, Compositio Math. **103** (1996), 319–350.

Mor98 P. Morton, *Galois groups of periodic points*, J. Algebra **201** (1998), 401–428.

Sil07 J. H. Silverman, *The arithmetic of dynamical systems*, Springer Graduate Texts in Mathematics, vol. 241 (Springer, Berlin, 2007).

Patrick Morton pmorton@math.iupui.edu
Department of Mathematical Sciences, Indiana University–Purdue University at Indianapolis,
402 N. Blackford St, LD 270, Indianapolis, Indiana 46202, USA

https://doi.org/10.1112/S0010437X1000480X Published online by Cambridge University Press