BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 46, Number 4, October 2009, Pages 703–704
S 0273-0979(09)01273-7
Article electronically published on July 21, 2009

ERRATA TO "THE CONSTRUCTION OF SOLVABLE POLYNOMIALS"

HAROLD M. EDWARDS

The following corrections need to be made to my article [1], which appeared in the July 2009 issue of the *Bulletin of the American Mathematical Society*.

1. Formula (2.3) in Theorem 2.1 should be stated in the equivalent form

$$G(x) = \prod_{j=1}^{\nu}(x^\mu - r_j r_{j-1}^{\delta} r_{j-2}^{\delta^2} \cdots r_{j-\nu+1}^{\delta^{\nu-1}})$$

in order to include the case $\nu = 1$. (When $\nu = 1$, the argument of footnote 12 fails and no δ satisfies the requirements of the theorem. When the formula is stated as above, no δ is called for when $\nu = 1$.)

In the special case $\nu = 1$, the definition of $G(x)$ in (5.2) should be replaced by $G(x) = x^\mu - s_0^\mu$, where s_0 is a nonzero Lagrange resolvent. (In this case, there is no m, but this $G(x)$ has the μ needed roots $\alpha^j s_0$.)

When $\nu = 1$, the assertion to be proved in Section 7 reduces to a tautology.

2. Proposition 4.1 contains a serious error that does not affect the rest of the paper. The formula $\alpha^j s_i \mapsto \alpha^j s_{i+\kappa}$ it gives for τ describes a permutation of the Lagrange resolvents, but *does not describe an automorphism of* Ω, so the proposition fails to provide the needed τ. (The τ constructed in the proof is an automorphism, but it does not combine with σ and η to generate the group.) Correction of the formula for τ implies corrections in the relations, but the main assertions remain:

Proposition. *Given an irreducible solvable polynomial $g(x)$ of prime degree μ with coefficients in an algebraic field K, let Ω be the field obtained by adjoining a μth root of unity $\alpha \neq 1$ to the splitting field of $g(x)$. The Galois group of Ω over K has order $\mu\nu\lambda$, where ν and λ are divisors of $\mu - 1$, and it is generated by automorphisms σ, τ and η, of order μ, ν and λ, respectively, that satisfy relations $\sigma\tau = \tau\sigma$, $\eta\tau = \tau\eta$, and $\eta\sigma = \sigma^\epsilon\eta$, where ϵ is an integer whose order* $\bmod \mu$ *is λ. As permutations of the Lagrange resolvents, such generators are described by $\sigma\colon \alpha^j s_i \mapsto \alpha^{j+\gamma^{-i}} s_i$, $\tau\colon \alpha^j s_i \mapsto \alpha^{j\delta} s_{i+\kappa}$, and $\eta\colon \alpha^j s_i \mapsto \alpha^{j\epsilon} s_i$, where γ is the primitive root* $\bmod \mu$ *used to define the Lagrange resolvents, where $\kappa = (\mu-1)/\nu$, and where $\delta \equiv \gamma^{-\kappa} \bmod \mu$.*

Proof. Let $\mathcal{G}$ be the Galois group of Ω over K. In Section 4, σ is defined to be an element of order μ in $\mathcal{G}$. As is shown, one can assume without loss of generality that it carries $\alpha^j s_i \mapsto \alpha^{j+\gamma^{-i}} s_i$, as in the statement of the proposition. Also in Section 4, η is defined to be a generator of the subgroup of $\mathcal{G}$ consisting of automorphisms that leave $s_1, s_2, \ldots, s_{\mu-1}$ fixed. As a permutation of the Lagrange resolvents, it is then given by the formula in the proposition.

Received by the editors July 6, 2009.
2000 *Mathematics Subject Classification.* Primary 11R32, 11R37, 11R18.

What is missing from Section 4 is the correct definition of τ. It is a generator of the subgroup of $\mathcal{G}$ consisting of automorphsims that leave the roots of $g(x)$ fixed. As is shown in Section 4, the most general permutation of the Lagrange resolvents that arises from an element of $\mathcal{G}$ has the form $\alpha^j s_i \mapsto \alpha^{aj-d\gamma^{-(i+b)}} s_{i+b}$ for some integers a, b, and d. The values of these integers are not arbitrary, however, but must be such that $\alpha \mapsto \alpha^a$ and $q_i \mapsto q_{ai\gamma^b+d}$ is an automorphism of Ω. (The letters a and b here replace the letters ϵ and λ that were injudiciously used in Section 4.) Since τ must carry $\alpha \mapsto \alpha^\delta$, where the order of δ mod μ is the order of the group generated by τ, a must be a number δ with this property. Since $\tau(q_i) = q_i$ for each i, d must be 0 and b must satisfy $a\gamma^b \equiv 1 \bmod \mu$. Thus, as a permutation of the $\alpha^j s_i$, τ has the form described in the proposition when ν is taken to be the order of the group of which τ is a generator.

The relations among σ, τ and η all follow from their formulas as permutations of the Lagrange resolvents, and it remains only to show that σ, τ and η generate $\mathcal{G}$, which amounts to saying that $\mathcal{G}$ has order $\mu\nu\lambda$. The $\mu(\mu-1)$ Lagrange resolvents $\alpha^j s_i$ are partitioned by σ and τ into κ orbits, each of length $\mu\nu$. (Two Lagrange resolvents $\alpha^j s_i$ and $\alpha^{j_1} s_{i_1}$ are in the same orbit if and only if $i \equiv i_1 \bmod \kappa$.) Each orbit, unless it consists of $\mu\nu$ zeros, contains the $\mu\nu$ roots of an irreducible (because $\mathcal{G}$ permutes its roots transitively) factor of $\prod(x^\mu - R_i)$ over K. As is shown in Section 4, two nonzero Lagrange resolvents $\alpha^j s_i$ and $\alpha^{j_1} s_{i_1}$ are equal only if $j \equiv j_1 \bmod \mu$ and $i \equiv i_1 \bmod (\mu-1)$, and adjunction of one nonzero s_i adjoins all of s_1, s_2, …, $s_{\mu-1}$. Therefore, $\prod(x^\mu - R_i)$ is a product of κ factors, each of which is irreducible of degree $\mu\nu$ over K, except that some (but not all) may be $x^{\mu\nu}$. Adjoining one root of one irreducible factor other than x is an extension of K of degree $\mu\nu$. The entire extension from K to Ω is reached by then adjoining α. The degree of this further extension is the order λ of η, so the degree of Ω over K is $\mu\nu \cdot \lambda$, and this is the order of $\mathcal{G}$, as was to be shown. □

Note that the corrected formula for τ does not change the effect of τ on the s_i, so the quantities r_i defined by (5.1) are still permuted cyclically by the Galois group.

3. The proof near the end of Section 7 that η and τ commute should state that the common value of $\tau\eta$ and $\eta\tau$ for any root $\alpha^j w_i$ of $G(x)$ is the unique μth root of w_{i+1}^μ that can be expressed rationally in terms of $\alpha^j w_i$, except when $K(w)$ contains a primitive μth root of unity; in the latter case, η is the identity and again $\eta\tau = \tau\eta$.

4. In formula (8.1), the exponent γ^{-i} should be replaced by a positive integer solution r of $r\gamma^i \equiv 1 \bmod \mu$. (For example, it could be replaced by the exponent γ_{-i} in formula (2.1). Since w_j^μ can be expressed in terms of r_j and absorbed into the coefficient $F_i(r_j)$, only the class of the exponent mod μ matters in the formula.)

5. Page 398 line 6, "he says" should be "Kronecker says."

6. Page 406, the third line from the bottom, the sentence beginning "This automorphism, call it τ," should begin, "This automorphism τ".

References

1. H. M. Edwards, *The construction of solvable polynomials,* Bull. Amer. Math. Soc., **46** (2009), 397–411.

Department of Mathematics, New York University, 251 Mercer St., New York, New York 10012