

## THE CONSTRUCTION OF SOLVABLE POLYNOMIALS

HAROLD M. EDWARDS

ABSTRACT. Although Leopold Kronecker’s 1853 paper “On equations that are algebraically solvable” is famous for containing his enunciation of the Kronecker-Weber theorem, its *main* theorem is an altogether different one, a theorem that reduces the problem of constructing *solvable* polynomials of prime degree  $\mu$  to the problem of constructing *cyclic* polynomials of degree  $\mu - 1$ . Kronecker’s statement of the theorem is sketchy, and he gives no proof at all. There seem to have been very few later treatments of the theorem, none of them very clear and none more recent than 1924. A corrected version and a full proof of the theorem are given. The main technique is a constructive version of Galois theory close to Galois’s own.

### 1. INTRODUCTION

Leopold Kronecker’s 1853 communication [11] to the Berlin Academy—his first publication<sup>1</sup> except for a note [10] he wrote as a student—is famous because it contains the assertion<sup>2</sup> that every abelian extension of the rationals is cyclotomic, the statement now known as the Kronecker-Weber theorem. The *main* theorem of the paper, however, is altogether different and has been largely<sup>3</sup> overlooked. It

---

Received by the editors November 21, 2008, and, in revised form, January 13, 2009.

2000 *Mathematics Subject Classification*. Primary 11R32, 11R37, 11R18.

*Key words and phrases*. Galois theory, solvable polynomials, Kronecker-Weber.

<sup>1</sup>For interesting material on the pre-history of Kronecker’s paper, see the letters from Kronecker to Dirichlet published in [16].

<sup>2</sup>Many authors describe it as a “conjecture”, probably because no proof is given and because it seems so improbable that Kronecker would have been able to prove it so early in the development of Galois theory. However, Kronecker calls it a “result” of theorems that he has stated in the paper and says it is true in full generality. Since he regarded the paper as a “preliminary communication”—he calls it a “*vorläufige Mitteilung*” on the last line of page 8 in volume 4 of his *Werke*—it is reasonable that he would leave out the proof. The mystery is that he never did give a proof and seems not even to have reacted when Heinrich Weber published [17] his proof 33 years later. Kronecker’s admission that he had achieved a “full solution” of his main problem only for  $\mu \not\equiv 1 \pmod{8}$  implies that he was confident both of the Kronecker-Weber theorem and of Theorem 2.1 below, except for the special case of the Kronecker-Weber theorem in which the degree is  $2^k$  for  $k > 2$ , which he expected he would soon prove. Some material on the Kronecker-Weber theorem may very well have been included among the many “wholly or partially completed” unpublished papers that Kurt Hensel, his scientific heir, mentions in the introduction to the first volume of Kronecker’s *Werke*. However, Hensel never fulfilled his promise to publish these papers, and they were lost in an accidental explosion in 1945 [3].

<sup>3</sup>I am aware of only the treatments by Weber [17], [18], Wiman [19], Netto [14], [15], and Fricke [8], the most recent of which was published in 1924. Moreover, I find them all difficult to understand, and none of them seems to me to cover the case in which, in the notation used below,  $\nu < \mu - 1$ . (As I explain below, I also find Kronecker’s treatment incorrect in this case.)

reduces the problem of constructing solvable polynomials of prime degree  $\mu$  to the problem of constructing cyclic polynomials of degree  $\mu - 1$ .

A few decades earlier, Niels Henrik Abel had proved his famous result that some quintic equations cannot be solved by radicals. As Kronecker points out in his introduction, however, Abel carried his study of solutions by radicals much further in [1], although he says this brief note—it is simply a long formula which August Crelle excerpted from one of Abel's letters and published in his *Journal für Mathematik* after Abel's death—was “little studied and quite specialized”. Abel told Crelle that the formula gives the solution of any quintic polynomial with rational coefficients that can be solved by radicals, but he gave no justification of this claim, let alone a proof. Kronecker states emphatically that he considers this direction of research—finding solutions of polynomials that can be solved by radicals—to be much more important and valuable than the research of Abel and Galois into finding criteria that determine whether a given polynomial can be solved by radicals. He points out, for example, that these criteria leave open the possibility that there are *no* polynomials of higher degree that are solvable by radicals other than very trivial examples.

Kronecker's goal was to generalize Abel's formula not only from degree 5 to arbitrary prime degree but also from polynomials with rational coefficients to polynomials with coefficients in any algebraic field. Thus, his goal was to give a formula that represented the most general quantity involving radicals that was a root of a polynomial of prime degree  $\mu$  with coefficients in a given field. Or, in the terms of modern field theory: Given a field, find an extension of it by a succession of adjunctions of radicals that contains a root of an irreducible polynomial of degree  $\mu$  with coefficients in the given field, and prove that the construction is general enough that every irreducible polynomial of degree  $\mu$  with coefficients in that field has—provided it can be solved by radicals—a root in a field constructed in the specified way.

The four quantities  $a, a_1, a_2, a_3$  that appear in Abel's formula in [1] are clearly the roots of an equation of degree 4 with rational coefficients. In a similar way, Kronecker's generalization to degree  $\mu$  makes use of  $\mu - 1$  auxiliary quantities that are the roots of a polynomial of degree  $\mu - 1$ , not of an *arbitrary* polynomial of degree  $\mu - 1$  but of one that is *cyclic* in the sense that its Galois group consists simply of the  $\mu - 1$  cyclic permutations of its roots. That is, Kronecker gives an algorithm that accepts as input a cyclic polynomial of degree  $\mu - 1$  and constructs an extension by radicals; he claims that the extension that is constructed contains a root of an irreducible polynomial of degree  $\mu$  and that any solvable irreducible polynomial of degree  $\mu$  has a root in a field obtained by the construction when a suitable input is used. He gives, however, no proof at all.

Terse as Kronecker's paper is, his method of constructing roots of solvable polynomials of prime degree with coefficients in a given algebraic field, though unproved, is rather clearly indicated except for the question of the possible reducibility of the auxiliary cyclic polynomial of degree  $\mu - 1$  used in the construction. In other words, he leaves unanswered the question of whether the roots  $r_1, r_2, \dots, r_{\mu-1}$  in cyclic order are distinct or, instead, consist of just  $\nu$  distinct roots  $r_1, r_2, \dots, r_\nu$  for some factor  $\nu$  of  $\mu - 1$ , after which they repeat  $r_{i+\nu} = r_i$ . Kronecker's algorithm

constructs a root when  $\nu = \mu - 1$ , but the construction of the *most general* root<sup>4</sup> of a solvable equation of degree  $\mu$  requires that the case  $\nu < \mu - 1$  be included. Fortunately, the needed modification of the algorithm is not hard to find.

Kronecker's construction is Theorem 2.1 below. The most important part of the theorem is of course the statement that *every* solvable polynomial has a root in a field that is constructed in this way. A formula for the most general root of a polynomial of degree  $\mu$  in a field obtained from the construction is given in Section 8; it agrees with Kronecker's formula when  $\nu = \mu - 1$ . Section 9 contains some remarks about the relation of this theorem to Kronecker's *Jugendtraum*.

2. THE THEOREM

Kronecker's point of departure is a formula of Abel that describes the roots of a solvable polynomial of prime degree  $\mu$  in terms of Lagrange resolvents. A Lagrange resolvent of a polynomial  $g(x)$  of degree  $\mu$  is an algebraic quantity<sup>5</sup> of the form  $\alpha q_1 + \alpha^2 q_2 + \dots + \alpha^{\mu-1} q_{\mu-1} + q_\mu$ , where  $\alpha \neq 1$  is a  $\mu$ th root of unity and  $q_1, q_2, \dots, q_\mu$  are the roots of  $g(x)$ . The use of Lagrange resolvents gives a uniform approach to the solution of equations of degree less than 5, but for larger degrees runs into difficulties because there are too many Lagrange resolvents: there are  $\mu!$  of them, one for each ordering of the  $q_i$ . However, Galois's theorem characterizing solvable polynomials of prime degree (see Section 4 below) singles out a preferred set of just  $\mu(\mu - 1)$  Lagrange resolvents in the case of a solvable  $g(x)$  of prime degree.

The analysis of the  $\mu(\mu - 1)$  Lagrange resolvents in this case is further aided by the fact that they have only  $\mu - 1$  distinct  $\mu$ th powers. These are the quantities Kronecker calls  $R_1, R_2, \dots, R_{\mu-1}$ . Galois had already observed (see his proof of his Proposition VII) that they are the roots of a *cyclic* polynomial, which means that when the  $R_j$  are put in a suitable order—if  $\gamma$  is a primitive root the<sup>6</sup> order

$$R_j = (\alpha q_{\gamma^j} + \alpha^2 q_{2\gamma^j} + \dots + \alpha^{\mu-1} q_{(\mu-1)\gamma^j} + q_\mu)^\mu$$

has this property—they are permuted cyclically by the Galois group.<sup>7</sup> In particular, the  $R_j$  can be expressed as radicals. If one could determine not just the  $R_j$  but their specific  $\mu$ th roots  $s_j = \alpha q_{\gamma^j} + \alpha^2 q_{2\gamma^j} + \dots + \alpha^{\mu-1} q_{(\mu-1)\gamma^j} + q_\mu$ , the formula<sup>8</sup>  $q_\mu = \frac{p_0 + s_1 + s_2 + \dots + s_{\mu-1}}{\mu}$ , where  $p_0$  is the quantity  $q_1 + q_2 + \dots + q_\mu$  in  $K$  (any symmetric function of the roots is in  $K$ ), would enable one to express a root of  $g(x)$  algebraically. More generally,  $p_0 + s_1 + s_2 + \dots + s_{\mu-1}$  would be the root of an irreducible polynomial of degree  $\mu$  for any  $p_0$  in  $K$ .

Kronecker's stated objective was to find the *most general* set of algebraic quantities  $s_1, s_2, \dots, s_{\mu-1}$  for which  $p_0 + s_1 + s_2 + \dots + s_{\mu-1}$  is a root of a solvable

<sup>4</sup>The solution of the equation  $x^5 = 2$  by Kronecker's method uses  $\nu = 1$  and the solution of the equation  $x^5 + 5x^3 + 5x + 14 = 0$  in Section 2 uses  $\nu = 2$ . I am unable to reconcile this fact with Kronecker's statement that his formula III, which works only when  $\nu = \mu - 1$ , covers all solvable polynomials. Similarly, it appears to me that Abel's formula does not provide roots of these two equations, which seems to belie his claim.

<sup>5</sup>Following Kronecker, I refer to elements of the base field and its algebraic extensions as "quantities".

<sup>6</sup>To say  $\gamma$  is a primitive root mod  $\mu$  means that  $\gamma^i \equiv 1 \pmod{\mu}$  if and only if  $i \equiv 0 \pmod{\mu - 1}$ .

<sup>7</sup>The Galois group may not act transitively on the  $R_j$  (for example, some  $R_j$  may be zero), so Kronecker's statement that  $\prod(x - R_j)$  is "abelian" is erroneous, because he goes on to define an abelian equation as one whose roots  $x_1, x_2, \dots, x_n$  can be expressed iteratively in terms of any one of them by a formula of the form  $x_{i+1} = \theta(x_i)$ .

<sup>8</sup>This formula follows from the fact that  $\sum_{k=1}^{\mu} \alpha^{bk}$  is  $\mu$  when  $b \equiv 0 \pmod{\mu}$ , 0 otherwise.

irreducible polynomial of degree  $\mu$  with coefficients in  $K$  whenever  $p_0$  is in  $K$ . Thus, he sought to give a formula for the most general algebraic quantity that can be a root of an irreducible solvable polynomial of prime degree  $\mu$ . Otherwise stated, he wanted not only to construct a field that would contain a root of a given polynomial of this type, but also, within that field, he wanted to find all quantities that were roots of such polynomials.

His enigmatic<sup>9</sup> answer is his formula

$$(2.1) \quad R_i = F(r_i)^\mu \cdot r_i^{\gamma-1} r_{i+1}^{\gamma-2} r_{i+2}^{\gamma-3} \cdots r_{i+\mu-2}$$

(formula III in his paper) in which  $\gamma_{-i}$  is the smallest positive solution of  $\gamma_{-i}\gamma^i \equiv 1 \pmod{\mu}$  and  $F(x)$  is a polynomial. I have found that to cover cases in which there are fewer than  $\mu - 1$  distinct roots  $r_i$ , this formula needs to be restated as

$$(2.2) \quad R_i = F(r_i)^\mu \cdot r_{i+1}^{\delta^{\nu-1}} r_{i+2}^{\delta^{\nu-2}} \cdots r_{i+\nu},$$

where  $\nu$  is a factor of  $\mu - 1$ , where the  $r_i$  are the roots of an irreducible cyclic polynomial of degree  $\nu$ , in their cyclic order, and  $\delta$  is an integer whose order mod  $\mu$  is  $\nu$ . When  $\nu = \mu - 1$ , the two formulas are essentially the same.<sup>10</sup>

**Theorem 2.1.** *Let  $\mu$  be a prime number and, for some factor  $\nu$  of  $\mu - 1$ , let  $f(x)$  be an irreducible cyclic polynomial of degree  $\nu$  with coefficients in an algebraic<sup>11</sup> field  $K$ . Let  $\delta$  be an integer whose order mod  $\mu$  is  $\nu$ , chosen in such a way<sup>12</sup> that  $\delta^\nu \not\equiv 1 \pmod{\mu^2}$ . Finally, let  $r_1, r_2, \dots, r_\nu$  be the roots of  $f(x)$  in a splitting field, listed in cyclic order. The polynomial defined by*

$$(2.3) \quad G(x) = \prod_{j=1}^{\nu} (x^\mu - r_{j+1}^{\delta^{\nu-1}} r_{j+2}^{\delta^{\nu-2}} \cdots r_{j+\nu})$$

(where  $r_i$  is defined for all positive integers  $i$  by the condition that  $r_i = r_j$  when  $i \equiv j \pmod{\nu}$ ) has coefficients in  $K$  because its coefficients are polynomials in  $r_1, r_2, \dots, r_\nu$  with coefficients in  $K$  that are unchanged by cyclic permutations of the  $r_i$ . If  $G(x)$  is irreducible<sup>13</sup> over  $K$ , then adjunction of one root  $w$  of  $G(x)$  to  $K$  gives an extension of  $K$  of degree  $\mu\nu$  which contains a root of a solvable irreducible polynomial of degree  $\mu$  with coefficients in  $K$ .

Conversely, any solvable irreducible polynomial of degree  $\mu$  with coefficients in  $K$  has a root in a field that is constructed in this way.

**Example 2.2.** Let  $\mu = 5$ ,  $\nu = 2$ ,  $\delta = 4$ , and let  $r_1$  and  $r_2$  be the roots  $1 \pm \sqrt{2}$  of  $f(x) = x^2 - 2x - 1$ . Then  $G(x) = (x^5 - r_1^4 r_2)(x^5 - r_2^4 r_1)$ ; because  $r_1 r_2 = -1$  and

<sup>9</sup>My paper [5] shows that as early as 1985 I was trying to understand formula (2.1).

<sup>10</sup>When  $\nu = \mu - 1$  and  $\delta = \gamma$  in (2.2), the ratio of  $r_i^{\gamma-1} r_{i+1}^{\gamma-2} r_{i+2}^{\gamma-3} \cdots r_{i+\mu-2}$  to  $r_i^{\delta^{\nu-1}} r_{i+1}^{\delta^{\nu-2}} \cdots r_{i+\nu-1}$  is a product of powers of the  $r_i$  in which all exponents are divisible by  $\mu$ , so it can be absorbed by the coefficient  $F(r_i)^\mu$ .

<sup>11</sup>As defined in [6], an algebraic field is an algebraic extension of finite degree of the field of rational functions in a finite number of indeterminates with integer coefficients. In particular, an algebraic number field is an algebraic field in which there are no indeterminates.

<sup>12</sup>To say that the order of  $\delta \pmod{\mu}$  is  $\nu$  means that  $\delta^i \equiv 1 \pmod{\mu}$  if and only if  $i \equiv 0 \pmod{\nu}$ . If  $\delta$  has order  $\nu \pmod{\mu}$  and  $\delta^\nu \equiv 1 \pmod{\mu^2}$ , then  $(\delta + \mu)^\nu = \delta^\nu + (\nu - 1)\delta^{\nu-1}\mu + \cdots \not\equiv 1 \pmod{\mu^2}$ , so if  $\delta$  does not have the required property  $\delta + \mu$  does.

<sup>13</sup>Kronecker does not impose this condition, but some such condition is necessary, as the case  $\mu = 3$ ,  $r_1 = \sqrt{2}$ ,  $r_2 = -\sqrt{2}$  shows. In this case  $G(x) = (x^3 - (\sqrt{2})^2(-\sqrt{2}))(x^3 + (-\sqrt{2})^2(\sqrt{2})) = x^6 - 8 = (x^2 - 2)(x^4 + 2x^2 + 4)$ . The degree of the splitting field of this  $G(x)$  is not divisible by 3, so it cannot contain a root of an irreducible cubic polynomial.

$r_1^3 + r_2^3 = 14$ , one easily finds  $G(x) = x^{10} + 14x^5 - 1$ . This polynomial is irreducible, and the theorem implies that adjunction of a root  $w$  of it to the field of rational numbers gives a field which contains quantities that are roots of irreducible quintics. As will be seen below, there is an automorphism of order  $\nu = 2$  of this field, and the roots of quintic polynomials are the quantities, other than constants, that are unremoved by this automorphism. The automorphism carries  $w \mapsto -\frac{1}{w}$ , so  $w - \frac{1}{w}$  is the root of a quintic. Paper-and-pencil computation in the field  $\mathbf{Q}(w)$  can be used to find that it is in fact a root of  $x^5 + 5x^3 + 5x + 14$ . Because  $w = \sqrt[5]{-(1 + \sqrt{2})^3}$ , this is a solution by radicals. The final statement of the theorem—the one that really counts—is that *any* irreducible polynomial of prime degree  $\mu$  that can be solved by radicals has a root in a field of this form for a suitable choice of  $\nu$ ,  $\delta$ , and  $r_1, r_2, \dots, r_\nu$ .

The proof of Theorem 2.1 will consist of an analysis, showing that a solvable irreducible polynomial of degree  $\mu$  has a root in a field constructed in this way (Section 5), and a synthesis, showing that any field constructed in this way contains quantities that are roots of irreducible polynomials of degree  $\mu$  (Section 7). (Such a polynomial is *ipso facto* solvable, because  $w$  can be expressed in terms of radicals.) Section 8 fulfills Kronecker's goal of finding *all* roots of irreducible polynomials of degree  $\mu$  in a field constructed by the method of Theorem 2.1.

### 3. CONSTRUCTIVE GALOIS THEORY

The truly “fundamental theorem of algebra” has nothing to do with complex numbers; it states simply that there is a valid way to compute with the roots of a given polynomial with rational coefficients (see [6] and [7]). In other words, the truly fundamental theorem is the construction of a *splitting field* of a given polynomial with rational coefficients.

An (algebraic) extension of the rational field  $\mathbf{Q}$ —the splitting field of a polynomial with rational coefficients is a particular case of such an extension—is described most concretely (see [6, p. 51]) by *adjunction relations* of the form  $\phi_1(q_1) = 0$ ,  $\phi_2(q_2, q_1) = 0$ ,  $\phi_3(q_3, q_2, q_1) = 0, \dots, \phi_n(q_n, q_{n-1}, \dots, q_2, q_1) = 0$ , in which each polynomial  $\phi_j(x, q_{j-1}, q_{j-2}, \dots, q_1)$  is monic in  $x$  with coefficients in  $\mathbf{Q}(q_{j-1}, q_{j-2}, \dots, q_1)$ , the field obtained by using the preceding relations to adjoin  $q_1, q_2, \dots, q_{j-1}$  to the rationals, and is *irreducible* over that field. If  $\nu_j$  is the degree of  $\phi_j$ , the  $j$ th relation can be used to replace  $q_j^{\nu_j}$  in any polynomial in  $q_1, q_2, \dots, q_n$  with  $q_j^{\nu_j} - \phi_j(q_j, q_{j-1}, \dots, q_1)$ , which is an “equal” polynomial whose degree in  $q_j$  is less than  $\nu_j$  by virtue of the assumption that  $\phi_j(x, q_{j-1}, q_{j-2}, \dots, q_1)$  is monic and of degree  $\nu_j$  in  $x$ . Repeated replacements of this sort can be used to show that every polynomial in  $q_1, q_2, \dots, q_n$  is “equal” to one in which the degree of  $q_j$  is less than  $\nu_j$  for each  $j$ . (First reduce the degree in  $q_n$ , then reduce the degree in  $q_{n-1}$  without increasing the degree in  $q_n$ , and so forth.) Such polynomials can be added in the usual way, and multiplied by multiplying in the usual way and using the adjunction relations to reduce the degrees. The assumption that the polynomials  $\phi_i$  are *irreducible* over their respective fields of coefficients guarantees that computations according to these rules describe a *field*. It is an algebraic extension of  $\mathbf{Q}$  of degree  $\nu_1 \nu_2 \cdots \nu_n$ , because that is the dimension of the vector space (over  $\mathbf{Q}$ ) of polynomials in  $q_1, q_2, \dots, q_n$  with coefficients in  $\mathbf{Q}$  in which the degree in  $q_j$  is less than  $\nu_j$  for each  $j$ .

Such adjunction relations can be used to describe any algebraic extension (of finite degree) of  $\mathbf{Q}$ . (In fact, by the theorem of the primitive element, every extension of  $\mathbf{Q}$  can be described by just *one* adjunction of this type.) The extension is **normal** if the number of its automorphisms is equal to the degree of the extension. Every extension is a subextension of a normal extension; for example, one can find a primitive element of the extension and adjoin *all* roots of the irreducible polynomial of which it is a root.

This method of describing a normal extension field  $\mathbf{Q}(q_1, q_2, \dots, q_n)$  by adjunction relations is very close to Galois's own conception of his theory. Adjunction of each  $q_j$  extends the field of "known" quantities. At the outset, only quantities in  $\mathbf{Q}$  are known. When  $q_1$  is adjoined, quantities in the field extension  $\mathbf{Q}(q_1)$  become known (these are the quantities rationally expressible in terms of  $q_1$ ) and the Galois group of the remaining field extension from  $\mathbf{Q}(q_1)$  to  $\mathbf{Q}(q_1, q_2, \dots, q_n)$  is reduced to a subgroup of index  $\nu_1$ , namely, the subgroup of those permutations that leave  $q_1$  fixed. Similarly, at the  $j$ th step, the field of known quantities  $\mathbf{Q}(q_1, q_2, \dots, q_{j-1})$  of degree  $\nu_1 \nu_2 \cdots \nu_{j-1}$  over  $\mathbf{Q}$  is extended to a field  $\mathbf{Q}(q_1, q_2, \dots, q_j)$  whose degree over  $\mathbf{Q}$  is  $\nu_j$  times as great, and the Galois group (the group of automorphisms of the field that leave the known quantities fixed) is reduced to a subgroup of index  $\nu_j$ . At the last step, the Galois group is reduced to the identity alone and all quantities in the field are "known".

An **algebraic number field** is an extension of  $\mathbf{Q}$  that can be described in this way. More generally, an **algebraic field** (see [6, p. 47]) is an extension of the field of rational functions, in one or more indeterminates, that can be described in a similar way by adjunction relations. (Galois allowed for such fields in the sense that some of his "known" quantities could be indeterminates.) Theorem 2.1 applies, as Kronecker intended, to arbitrary algebraic fields  $K$ .

#### 4. THE ACTION OF THE GALOIS GROUP ON THE LAGRANGE RESOLVENTS

Galois proved in [9, Proposition VII] that *a polynomial  $g(x)$  of prime degree  $\mu$  with coefficients in an algebraic field  $K$  is solvable if and only if its roots  $q_1, q_2, \dots, q_\mu$  can be listed in such a way that every permutation of them that is effected by its Galois group has the form  $q_i \mapsto q_{ai+b}$  for some integers  $a$  and  $b$ . (Here  $q_i$  is of course defined for all integer values of  $i$  by the condition that  $q_i = q_j$  whenever  $i \equiv j \pmod{\mu}$ . Because  $q_i \mapsto q_{ai+b}$  is a permutation,  $a$  must be nonzero mod  $\mu$ .)*

The Lagrange resolvents of  $g(x)$  lie in a (normally) larger field than the splitting field of  $g(x)$  over  $K$ , namely, the field  $\Omega$  obtained by adjoining a  $\mu$ th root of unity  $\alpha \neq 1$  to that splitting field. Galois's theorem shows that a *solvable* equation of prime degree  $\mu$  has  $\mu(\mu - 1)$  special Lagrange resolvents (they are quantities in  $\Omega$ ), namely,  $s_{a,b} = \sum_{k=1}^{\mu} \alpha^k q_{ak+b}$  in which  $a = 1, 2, \dots, \mu - 1$  and  $b = 1, 2, \dots, \mu$ . In what follows, only these  $\mu(\mu - 1)$  quantities (they need not be distinct) will be called Lagrange resolvents of  $g(x)$ . They are independent of the way in which the roots  $q_1, q_2, \dots, q_\mu$  are listed, provided they are listed in such a way that the permutations in the Galois group of  $g(x)$  all have the form  $q_i \mapsto q_{ai+b}$ .

The polynomial  $\prod(x - s_{a,b})$  is  $\prod_{a=1}^{\mu-1} (x^\mu - s_{a,0}^\mu)$  because  $x^\mu - s^\mu = \prod_{j=1}^{\mu} (x - \alpha^j s)$  and  $s_{a,b} = \sum_{k=1}^{\mu} \alpha^k q_{ak+b} = \sum_{l=1}^{\mu} \alpha^{a^{-1}(l-b)} q_l = \alpha^{-a^{-1}b} \sum_l \alpha^{a^{-1}l} q_l = \alpha^{-a^{-1}b} s_{a,0}$  (where  $a^{-1}$  denotes an integer that is reciprocal to  $a$  mod  $\mu$ ). It is convenient to reorder the factors of  $\prod(x^\mu - s_{a,0}^\mu)$  by setting  $s_i = s_{\gamma^i, 0}$  for some primitive root  $\gamma$  mod  $\mu$ , which also serves to define  $s_i$  for all  $i$  in such a way that  $s_i = s_j$  whenever

$i \equiv j \pmod{\mu - 1}$ . Each Lagrange resolvent can be written in the form  $\alpha^j s_i$  and the polynomial  $\prod(x - s_{a,b})$  takes the form  $\prod_{i=1}^{\mu-1}(x^\mu - s_i^\mu)$ , or, in the notation of Section 2, the form  $\prod_{i=1}^{\mu-1}(x^\mu - R_i)$ .

**Proposition 4.1.** *Given an irreducible solvable polynomial  $g(x)$  of prime degree  $\mu$  with coefficients in an algebraic field  $K$ , let  $\Omega$  be the field obtained by adjoining a  $\mu$ th root of unity  $\alpha \neq 1$  to the splitting field of  $g(x)$ . The Galois group of  $\Omega$  over  $K$  has order  $\mu\nu\lambda$ , where  $\nu$  and  $\lambda$  are divisors of  $\mu - 1$ . It is generated by automorphisms  $\sigma$ ,  $\tau$ , and  $\eta$ , of order  $\mu$ ,  $\nu$ , and  $\lambda$ , respectively, that satisfy the relations  $\eta\sigma = \sigma\eta$ ,  $\eta\tau = \tau\eta$ , and  $\tau\sigma = \sigma^\delta\tau$ , where  $\delta$  is an integer whose order mod  $\mu$  is  $\nu$ . Specifically, as permutations of the Lagrange resolvents, these generators can be taken to be  $\sigma: \alpha^j s_i \mapsto \alpha^{j+\gamma^{-i}} s_i$ ,  $\tau: \alpha^j s_i \mapsto \alpha^j s_{i+\kappa}$  and  $\eta: \alpha^j s_i \mapsto \alpha^{\epsilon j} s_i$ , where  $\gamma$  is the primitive root mod  $\mu$  used in the definition of the  $s_i$ ,  $\kappa = (\mu - 1)/\nu$ , and  $\epsilon$  is a number whose order mod  $\mu$  is  $\lambda$ . (With these definitions,  $\delta \equiv \gamma^\kappa \pmod{\mu}$ .)*

*Proof.* The formula  $\mu q_k = p_0 + \sum_{i=1}^{\mu-1} \alpha^{-k\gamma^{-i}} s_i$ , where  $p_0 = q_1 + q_2 + \dots + q_\mu$  is in  $K$ , shows that the splitting field of  $g(x)$  is contained in the field obtained by adjoining  $\alpha$ ,  $s_1, s_2, \dots, s_{\mu-1}$  to  $K$ . Since the  $q_i$  are not in  $K$ , at least one  $s_i$  is nonzero, so  $\alpha = \alpha s_i / s_i$  is a quotient of Lagrange resolvents, which implies that all of  $\Omega$  lies in the field obtained by adjoining the Lagrange resolvents to  $K$ . In other words,  $\Omega$  is the splitting field of the polynomial  $\prod_{i=1}^{\mu-1}(x^\mu - R_i)$  with coefficients in  $K$  of which the Lagrange resolvents are the roots. In particular, the Galois group of  $\Omega$  over  $K$  can be described as a group of permutations of the Lagrange resolvents  $\alpha^j s_i$ .

Let  $\mathcal{G}$  be the Galois group of  $\Omega$  over  $K$  and let  $\mathcal{G}_0$  be the subgroup containing the automorphisms that leave  $\alpha$  fixed. In other words,  $\mathcal{G}_0$  is the subgroup to which  $\mathcal{G}$  is reduced by the adjunction of  $\alpha$ .

The Galois group of  $g(x)$  over  $K$  contains an element of order  $\mu$  because it is a subgroup of the group of  $\mu(\mu - 1)$  permutations of the form  $q_i \mapsto q_{ai+b}$  that acts transitively on the  $q_i$ . The elements of order  $\mu$  necessarily act on the roots as  $q_i \mapsto q_{i+b}$ , where  $b \not\equiv 0 \pmod{\mu}$ , and each such permutation is a power of any other. Therefore, the Galois group of  $g(x)$  over  $K$  contains an element of order  $\mu$  that carries  $q_i \mapsto q_{i-1}$ . Because  $\Omega$  is a normal extension of the splitting field of  $g(x)$ , this automorphism of the splitting field of  $g(x)$  over  $K$  extends to an automorphism of  $\Omega$  over  $K$ . This extension, which is in  $\mathcal{G}$ , must be in  $\mathcal{G}_0$ , because its action on the  $\mu - 1$  powers of  $\alpha$  other than 1 partitions them into orbits whose lengths must divide  $\mu$ , so the orbits must all be of length one.

In short,  $\mathcal{G}_0$  contains an element of order  $\mu$  that carries  $q_i \mapsto q_{i-1}$ , call it  $\sigma$ . It carries  $\alpha^j s_i = \alpha^j \sum_{k=1}^{\mu} \alpha^k s_{k\gamma^i}$  to  $\alpha^j \sum_{k=1}^{\mu} \alpha^k s_{k\gamma^{i-1}} = \alpha^j s_{\gamma^{i-1}} = \alpha^j \alpha^{\gamma^{-i}} s_{\gamma^i, 0} = \alpha^{j+\gamma^{-i}} s_i$ , which is the formula in the statement of the theorem. (It was shown above that  $s_{a,b} = \alpha^{-a^{-1}b} s_{a,0}$ .)

By elementary group theory, the group of permutations  $q_i \mapsto q_{ai+b}$  has just one subgroup of order  $\mu\nu$  for each factor  $\nu$  of  $\mu - 1$ , namely, the subgroup generated by  $\sigma: q_i \mapsto q_{i-1}$  and  $\tau: q_i \mapsto q_{\gamma^\kappa i}$ , where  $\kappa = (\mu - 1)/\nu$ . Therefore,  $\mathcal{G}_0$  is generated by  $\sigma$  and the automorphism  $\tau$  of  $\Omega$  that is determined by  $\tau: \alpha \mapsto \alpha$  and  $\tau: q_i \mapsto q_{i\gamma^\kappa}$ , where  $\kappa$  is determined in this way. Since the action of  $\tau$  on the Lagrange resolvents is  $\alpha^j s_i \mapsto \alpha^j \sum \alpha^k q_{k\gamma^i\gamma^\kappa} = \alpha^j s_{i+\kappa}$ , this proves that  $\mathcal{G}_0$  is the group of automorphisms of  $\Omega$  over  $K$  generated by the automorphisms  $\sigma$  and  $\tau$  described in the proposition.

Lagrange resolvents  $\alpha^j s_i$  and  $\alpha^l s_k$  that are nonzero are equal only if they are identical, which is to say only if  $j \equiv l \pmod{\mu}$  and  $i \equiv k \pmod{\mu-1}$ , as can be seen in the following way. Application of  $\sigma$  to an equation  $\alpha^j s_i = \alpha^l s_k$  gives  $\alpha^{\gamma^{-i}} \alpha^j s_i = \alpha^{\gamma^{-k}} \alpha^l s_k$ . Provided  $\alpha^j s_i = \alpha^l s_k$  is nonzero, the new equation can be divided by the original equation to find  $\alpha^{\gamma^{-i}} = \alpha^{\gamma^{-k}}$ , which implies  $\gamma^{-i} \equiv \gamma^{-k} \pmod{\mu}$  and  $i \equiv k \pmod{\mu-1}$ . Thus,  $s_i = s_k$  and  $\alpha^j = \alpha^l$ , which implies  $j \equiv l \pmod{\mu}$ , as was to be shown.

An element of  $\mathcal{G}$  carries  $\alpha \mapsto \alpha^\epsilon$  and  $q_i \mapsto q_{ci+d}$  for some integers  $\epsilon$ ,  $c$ , and  $d$ , where  $c \not\equiv 0 \pmod{\mu}$ . It then carries  $\alpha^j s_i$  to

$$\alpha^{\epsilon j} \sum_{k=1}^{\mu} \alpha^{\epsilon k} q_{ck\gamma^i+d} = \alpha^{\epsilon j} \sum_{l=1}^{\mu} \alpha^l q_{\epsilon^{-1}cl\gamma^i+d} = \alpha^{\epsilon j} \sum_{l=1}^{\mu} \alpha^l q_{l\gamma^{i+\lambda}+d}$$

when  $\lambda$  satisfies  $\epsilon^{-1}c \equiv \gamma^\lambda \pmod{\mu}$ . This is  $\alpha^{\epsilon j} s_{\gamma^{i+\lambda},d} = \alpha^{\epsilon j} \alpha^{-d\gamma^{-(i+\lambda)}} s_{i+\lambda}$ . An element of  $\mathcal{G}$  that leaves  $s_i$  unchanged for one value of  $i$  for which  $s_i \neq 0$  then satisfies  $\alpha^{-d\gamma^{-(i+\lambda)}} s_{i+\lambda} = s_i$ , so both  $d \equiv 0 \pmod{\mu}$  and  $\lambda \equiv 0 \pmod{\mu-1}$ , which implies that the element leaves  $s_i$  fixed for every  $i$ . Therefore, by Galois's fundamental theorem, the adjunction of one nonzero  $s_i$  to  $K$  gives a field  $K(s)$  that includes all of the Lagrange resolvents  $\alpha^j s_i$  in which  $j = 0$ . (As was noted above, at least one of  $s_1, s_2, \dots, s_{\mu-1}$  must be nonzero because  $s_1 + s_2 + \dots + s_\mu$  is not in  $K$ .) Since  $q_\mu = (p_0 + s_1 + s_2 + \dots + s_{\mu-1})/\mu$ ,  $K(s)$  also contains a root of  $g(x)$ .

The Galois group of  $\Omega$  over  $K(s)$  is the subgroup of  $\mathcal{G}$  containing elements that leave all of the  $s_i$  fixed. Such an element carries  $\alpha^j s_i \mapsto \alpha^{\epsilon j} s_i$  for some  $\epsilon$ . As was shown above,  $\Omega$  is contained in the field obtained by adjoining  $\alpha$  to  $K(s)$ , so the Galois group of  $\Omega$  over  $K(s)$  is a subgroup of the Galois group of  $x^\mu - 1$  over  $\mathbf{Q}$ , which is a cyclic group of order  $\mu - 1$ . Therefore, it is cyclic of order  $\lambda$  for some factor  $\lambda$  of  $\mu - 1$ , which is to say that it is generated by a single automorphism  $\eta$  of order  $\lambda$  that carries  $\alpha^j s_i \mapsto \alpha^{\epsilon j} s_i$ , and the proposition follows.  $\square$

**Corollary 4.1.** *Adjunction of one nonzero Lagrange resolvent of  $g(x)$  to  $K$  gives a field in which  $g(x)$  has a root.*

*Proof.* This was shown directly in the course of the proof, but it also follows from the proposition, because, provided  $s_i \neq 0$ , the elements of the Galois group that leave  $s_i$  unmoved are simply the powers of  $\tau$ , which also leave the root  $q_\mu = (p_0 + s_1 + s_2 + \dots + s_{\mu-1})/\mu$  of  $g(x)$  unmoved.  $\square$

## 5. CONSTRUCTION OF A ROOT OF A GIVEN IRREDUCIBLE SOLVABLE POLYNOMIAL OF DEGREE $\mu$

As is shown in Section 4, adjunction of a nonzero Lagrange resolvent of  $g(x)$  to  $K$  constructs a field in which  $g(x)$  has a root. Therefore, a field in which  $g(x)$  has a root can be constructed by adjoining to  $K$  the  $\mu$ th root of one of the quantities  $R_i = s_i^\mu$ , provided  $R_i \neq 0$ . Kronecker's mysterious formula (2.1) asserts that such a field can be constructed by adjoining first a root  $r_i$  of a suitably chosen cyclic equation of degree  $\mu - 1$ , and then a  $\mu$ th root of a specific quantity in the field that is obtained in this way (namely,  $r_i^{\gamma-1} r_{i+1}^{\gamma-2} r_{i+2}^{\gamma-3} \dots r_{i+\mu-2}$ ). Thus, (2.1) serves a dual function: It specifies both a cyclic extension and a quantity in that extension of which a  $\mu$ th root is to be adjoined. Formula (2.2) does the same in the general case in which  $\nu$  is a factor of  $\mu - 1$ , not necessarily  $\mu - 1$  itself; it specifies a cyclic

extension of degree  $\nu$  and an element of that extension of which a  $\mu$ th root is to be adjoined to obtain a field that contains a root of  $g(x)$ .

In fact, when the quantities  $r_i$  are defined by<sup>14</sup>

$$(5.1) \quad r_i = \frac{s_{i\kappa}^\delta}{s_{(i+1)\kappa}} \quad (i = 1, 2, \dots, \nu),$$

where  $\delta \equiv \gamma^{-\kappa} \pmod{\mu}$ , one finds that the  $r_i$  are permuted cyclically by  $\mathcal{G}$  (because  $\eta$  leaves the  $r_i$  unchanged,  $\tau$  carries  $r_i$  to  $r_{i+1}$ , and  $\sigma$  multiplies  $r_i$  by  $\alpha^{\delta\gamma^{-i\kappa}}/\alpha^{\gamma^{-(i+1)\kappa}} = 1$ , which is to say that  $\sigma$  leaves  $r_i$  unchanged) and

$$r_{i+1}^{\delta^{\nu-1}} r_{i+2}^{\delta^{\nu-2}} \cdots r_{i+\nu} = \frac{s_{(i+1)\kappa}^{\delta^\nu}}{s_{(i+2)\kappa}^{\delta^{\nu-1}}} \cdot \frac{s_{(i+2)\kappa}^{\delta^{\nu-1}}}{s_{(i+3)\kappa}^{\delta^{\nu-2}}} \cdots \frac{s_{(i+\nu)\kappa}^\delta}{s_{(i+1+\nu)\kappa}} = s_{(i+1)\kappa}^{\delta^{\nu-1}}$$

is a  $\mu$ th power because the exponent  $\delta^{\nu-1}$  on the right is divisible by  $\mu$ . Specifically, this quantity is the  $\mu$ th power of  $s_{(i+1)\kappa}^m$ , where  $m$  is the integer  $(\delta^{\nu-1})/\mu$ . Thus, the polynomial

$$(5.2) \quad G(x) = \prod_{i=1}^{\nu} (x^\mu - r_{i+1}^{\delta^{\nu-1}} r_{i+2}^{\delta^{\nu-2}} \cdots r_{i+\nu})$$

of degree  $\mu\nu$  with coefficients in  $K$  has  $\mu\nu$  nonzero roots  $\alpha^j s_{i\kappa}^m$  in  $\Omega$ .

If, as is stipulated in Theorem 2.1,  $\delta^\kappa$  is not 1 mod  $\mu^2$ , these  $\mu\nu$  roots  $\alpha^j s_{i\kappa}^m$  of  $G(x)$  are *distinct* by virtue of the assumption that  $m$  is relatively prime to  $\mu$ , because application of  $\sigma$  to an equation  $\alpha^j s_{i\kappa}^m = \alpha^l s_{k\kappa}^m$  multiplies the left side by  $\alpha^{m\gamma^{-i\kappa}}$  and the right by  $\alpha^{m\gamma^{-k\kappa}}$ , which implies, unless both sides are zero, that  $m\gamma^{-i\kappa} \equiv m\gamma^{-k\kappa} \pmod{\mu}$ , from which it follows that  $i\kappa \equiv k\kappa \pmod{\mu-1}$  and therefore that  $s_{i\kappa} = s_{k\kappa}$  and  $\alpha^j = \alpha^l$ . Moreover,  $\mathcal{G}$  acts transitively on the roots of  $G(x)$  because it acts transitively on the  $R_{i\kappa}$  (by the definition of  $\kappa$ ) and it acts transitively on the  $\mu$ th roots  $\alpha^j s_{i\kappa}^m$  of any  $R_{i\kappa}$  (because  $\sigma$  acts transitively on these roots).

Therefore, *the polynomial  $G(x)$  defined by (5.2) is irreducible over  $K$* . In particular, the quantities  $r_1, r_2, \dots, r_\nu$  are distinct (otherwise,  $G(x)$  would have repeated factors), so the cyclic polynomial of degree  $\nu$  with coefficients in  $K$  of which the  $r_i$  are roots is also irreducible. Therefore,  $G(x)$  is determined by formula (2.3) when  $f(x)$  is the polynomial of which the  $r_i$  are the roots, provided the  $r_i$  are ordered as above and  $\delta = \gamma^{-\kappa}$ .

The elements of  $\Omega$  that can be expressed rationally in terms of a root  $w = s_{i\kappa}^m$  of  $G(x)$  are, by Galois's fundamental theorem, those that are unmoved by the elements of the Galois group that leave  $w$  unmoved. These are simply the powers of  $\eta$ , which are also the elements of  $\mathcal{G}$  that leave the  $s_i$  unmoved. Thus, adjunction of  $w$  gives the field  $K(s)$ , which contains a root of  $g(x)$ ; since this field is constructed as in Theorem 2.1, the analysis is complete.

---

<sup>14</sup>In this definition it is assumed that  $s_0 \neq 0$ , which implies that  $s_{i\kappa} \neq 0$  for all  $i$ . There is no loss of generality in this assumption, because the Lagrange resolvents all have the form  $\sum \alpha^k q_k$  for some cyclic order of the  $q_i$ , so this order can be chosen to give any one of the  $\mu(\mu-1)$  Lagrange resolvents the label  $s_0$ .

6. A CLASSICAL LEMMA ABOUT  $\mu$ TH ROOTS

The synthesis—the proof that a field constructed by the method of Theorem 2.1 contains a root of an irreducible solvable polynomial of degree  $\mu$ —will make use of:

**Lemma 6.1.** *Let  $K$  be an algebraic field. When  $\mu$  is prime, a polynomial of the form  $x^\mu - c$  with coefficients in  $K$  is reducible over  $K$  only if it has a linear factor, or, what is the same, only if  $c$  is a  $\mu$ th power in  $K$ .*

This lemma is proved in a much later work [12] of Kronecker, but since it appears at the very beginning of that work, and since the work is an exposition of the work of Abel on algebraic equations, it is reasonable to suppose that the lemma was familiar to Kronecker in 1853. Today it can be regarded as an exercise in Galois theory (see [4, Exercise 6, p. 98 with an answer on p. 141] or [2, p. 85]).

## 7. PROOF OF THE FIRST STATEMENT OF THEOREM 2.1

Let  $G(x)$  be a polynomial of the form (2.3), where  $\mu$  is prime,  $f(x)$  is an irreducible cyclic polynomial with coefficients in an algebraic field  $K$  whose degree  $\nu$  divides  $\mu - 1$ , and  $\delta$  is a number whose order mod  $\mu$  is  $\nu$  but for which  $\delta^\nu \not\equiv 1 \pmod{\mu^2}$ . It is to be shown that if  $G(x)$  is irreducible, then the field obtained by adjoining one root  $w$  of  $G(x)$  contains a root of an irreducible polynomial of degree  $\mu$ .

The natural way to adjoin one root of  $G(x)$  to  $K$  is by means of two adjunction relations

$$(7.1) \quad \begin{aligned} f(r) &= 0, \\ w^\mu - r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots r_{\nu-1}^\delta r_\nu &= 0, \end{aligned}$$

where, in the second relation, use is made of the assumption that  $f(x)$  is cyclic to construct roots  $r_1, r_2, \dots, r_\nu$  of  $f(x)$  in  $K(r)$  that are permuted cyclically by the Galois group of  $f(x)$ .

If  $r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots r_{\nu-1}^\delta r_\nu$  were a  $\mu$ th power in  $K(r)$ , say  $r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots r_{\nu-1}^\delta r_\nu = \zeta^\mu$  for some  $\zeta$  in  $K(r)$ , then  $x - \zeta$  would be a factor of the first factor of  $G(x)$  and each of the  $\nu$  conjugates of  $x - \zeta$  under the Galois group of  $f(x)$  would be a factor of one of the  $\nu$  factors of  $G(x)$ , so the product of these  $\nu$  linear polynomials with coefficients in  $K(r)$  would be a factor of  $G(x)$  of degree  $\nu$  with coefficients in  $K$ , contrary to the assumption that  $G(x)$  (a polynomial of degree  $\nu\mu$ ) is irreducible.

Therefore, the relations (7.1) are in fact adjunction relations by virtue of the lemma of Section 6 and the assumption that  $G(x)$  is irreducible. Let  $K(r, w)$  denote the field they define, and let the  $r$  in this field be identified with  $r_1$  in the second adjunction relation. The rules  $r \mapsto r_2$  and  $w \mapsto w^\delta / r^m$ , where  $m = (\delta^\nu - 1) / \mu$ , define an automorphism of  $K(r, w)$ , call it  $\tau$ , as can be seen in the following way. The automorphism of  $K(r)$  that carries  $r_i \mapsto r_{i+1}$  carries the quantity  $r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots r_{\nu-1}^\delta r_\nu$  in the second relation to  $r_2^{\delta^{\nu-1}} r_3^{\delta^{\nu-2}} \cdots r_\nu^\delta \cdot r_1$ , so what is to be shown is that  $w^\delta / r^m$  is a  $\mu$ th root of  $r_2^{\delta^{\nu-1}} r_3^{\delta^{\nu-2}} \cdots r_\nu^\delta \cdot r_1$ , which follows from direct computation:

$$\left(\frac{w^\delta}{r^m}\right)^\mu = \frac{(r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots r_\nu)^\delta}{r^{(\delta^\nu-1)}} = \frac{r_1^{\delta^\nu} r_2^{\delta^{\nu-1}} \cdots r_\nu^\delta}{r_1^{\delta^\nu} \cdot r_1^{-1}} = r_2^{\delta^{\nu-1}} r_3^{\delta^{\nu-2}} \cdots r_\nu^\delta \cdot r_1.$$

This automorphism, call it  $\tau$ , has order  $\nu$  as can be seen in the following way. Since  $\tau$  permutes the  $r_i$  cyclically, its  $\nu$ th power is the identity on  $K(r)$ , and no lower power is the identity on  $K(r)$ . What is to be shown, therefore, is that  $\tau^\nu(w) = w$ ,

which is another direct computation: Let  $w_1$  be  $w$  and let  $w_i$  be  $\tau(w_{i-1})$  for  $i = 2, 3, \dots$ . Then  $w_2 = \frac{w^\delta}{r_1^m}$ ,  $w_3 = \frac{w^{\delta^2}}{r_1^m r_2^m}$ ,  $w_4 = \frac{w^{\delta^3}}{r_1^m r_2^m r_3^m}, \dots$ ,

$$w_{\nu+1} = \frac{w^{\delta^\nu}}{(r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \dots r_\nu)^m} = \frac{w^{\delta^\nu}}{w^{\mu m}} = w_1.$$

In particular, the polynomial  $G(x)$  with coefficients in  $K$  defined by (2.3) has  $\nu$  roots  $w_1, w_2, \dots, w_\nu$  in  $K(r, w)$ . The Galois group of  $G(x)$  is the group of automorphisms of the splitting field of  $G(x)$ . Such a splitting field is obtained by adding another adjunction relation to (7.1), namely,

$$(7.2) \quad \begin{aligned} f(r) &= 0, \\ w^\mu - r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \dots r_{\nu-1}^\delta r_\nu &= 0, \\ h(\alpha, r, w) &= 0, \end{aligned}$$

where  $h(x, r, w)$  is one of the irreducible factors of  $x^\mu - 1$  over  $K(r, w)$  other than the factor  $x - 1$ . (If  $K(r, w)$  already contains an  $\alpha$ , then  $h(x, r, w)$  has degree 1 and the fields defined by (7.1) and (7.2) coincide.)

The extension of  $K$  defined by (7.2), call it  $\Omega$ , is a normal extension, as can be seen in the following way. An automorphism of  $\Omega$  over  $K$  must carry  $r$  to one of the  $\nu$  distinct roots  $r_i$  of  $f(x)$  in  $K(r)$ . If the image of  $r$  is  $r_i$ , then the image of  $w$  must be a  $\mu$ th root of  $r_i^{\delta^{\nu-1}} r_{i+1}^{\delta^{\nu-2}} \dots r_{i-2}^\delta r_{i-1}$  in  $\Omega$ , of which there are  $\mu$ , namely, those given by the formula  $\alpha^j w_i$  for  $j = 1, 2, \dots, \mu$ . Finally, if the image of  $r$  is  $r_i$  and the image of  $w$  is  $\alpha^l w_i$ , then the image of  $\alpha$  must be a root of  $h(x, r_i, \alpha^l w_i)$ , of which there are exactly  $\lambda = \deg h$  in  $\Omega$ . (The Galois group of the extension  $\mathbf{Q}(\alpha)$  is cyclic of order  $\mu - 1$ ; specifically, it is generated by the permutation  $\alpha \mapsto \alpha^\gamma$  of the roots of  $x^\mu - 1$  other than 1. Adjunction of generators of  $K$  (including, possibly, a finite number of indeterminates, which obviously do not affect the factorization of  $x^\mu - 1$ ) followed by adjunction of  $r$  and  $w$  reduces this Galois group, if it reduces it at all, to the cyclic subgroup whose order is the degree of the irreducible factors of  $x^\mu - 1$  over  $K(r, w)$  other than  $x - 1$ . In particular, these factors all have the same degree  $\lambda$  and they partition the powers of  $\alpha$  other than 1 into orbits of length  $\lambda$ .) Thus, there are at most  $\nu\mu\lambda$  automorphisms of  $\Omega$  over  $K$ .

The  $\mu\nu$  roots  $\alpha^j w_i$  (where  $j = 1, 2, \dots, \mu$  and  $i = 1, 2, \dots, \nu$ ) of  $G(x)$  in  $\Omega$  are distinct, because a multiple root would imply that  $G(x)$  had a nontrivial divisor in common with its derivative, which is impossible because  $G(x)$  is irreducible by assumption. For each of these  $\mu\nu$  roots  $\alpha^j w_i$  of  $G(x)$ , there are  $\lambda$  automorphisms of  $\Omega$  over  $K$  that carry  $w$  to  $\alpha^j w_i$ , namely, those that carry  $(r, w, \alpha)$  to  $(r_i, \alpha^j w_i, \alpha^k)$ , where  $\alpha^k$  is one of the  $\lambda$  roots of  $h(x, r_i, \alpha^j w_i)$ . Therefore, the number of automorphisms of  $\Omega$  over  $K$  is equal to the degree  $\mu\nu\lambda$  of  $\Omega$  over  $K$ , so  $\Omega$  is a normal extension of  $K$ .

Also,  $\Omega$  is a *solvable* extension of  $K$ —it can be accomplished by the adjunction of radicals—because the second adjunction *is* a radical, and the Galois groups of the other two adjunctions are abelian.

Thus, it remains only to show that the subfield of  $\Omega$  obtained by adjoining one root  $w$  of  $G(x)$  to  $K$  contains a root of an irreducible polynomial of degree  $\mu$ . Let  $\eta$  be a generator of the subgroup of  $\mathcal{G}$  that leaves all elements of  $K(w) = K(r, w)$  fixed. Since  $\eta$  must have order  $\lambda$  and must permute the powers of  $\alpha$ , it must have the form  $\alpha^j w_i \mapsto \alpha^{j\epsilon} w_i$ , where  $\epsilon$  is an integer whose order mod  $\mu$  is  $\lambda$ . Since

$\eta$  commutes with  $\tau$  (their composition, in either order, carries  $\alpha^j w_i \mapsto \alpha^{j\epsilon} w_{i+1}$ ), together with  $\tau$  it generates a commutative subgroup  $\mathcal{G}$  of order  $\nu\lambda$ , call it  $\mathcal{H}$ .

Since  $\mathcal{H}$  has index  $\mu$  in the Galois group, it corresponds to a subfield of  $\Omega$  whose degree over  $K$  is  $\mu$ . Such a subfield adjoins to  $K$  one root of an irreducible polynomial of degree  $\mu$  with coefficients in  $K$ . Since it is contained in  $K(w)$  (which corresponds to the subgroup of  $\mathcal{H}$  of order  $\lambda$  generated by  $\eta$ ),  $K(w)$  must contain a root of an irreducible polynomial of degree  $\mu$ , which completes the proof of Theorem 2.1.  $\square$

## 8. THE FORM OF THE ROOTS

Theorem 2.1 reduces the problem of constructing a splitting field of the most general irreducible solvable polynomial of degree  $\mu$  with coefficients in  $K$  to the problem of constructing the most general irreducible cyclic polynomial with coefficients in  $K$  whose degree divides  $\mu - 1$ . But Kronecker's goal was not just to construct the most general *splitting field*, but also to find the most general *root* of an irreducible polynomial of degree  $\mu$  within that field.

Theorem 2.1 states that every solvable irreducible polynomial of prime degree  $\mu$  has a root in a field of the form  $K(w)$  obtained by adjoining one root  $w$  of an irreducible polynomial of the form  $G(x)$  to  $K$ . The polynomial then has  $\mu$  roots in the splitting field  $\Omega$  of  $G(x)$ , namely, the quantities in the orbit under  $\sigma$  of the root in  $K(w)$ . The elements of the Galois group that leave this root unmoved form a subgroup of index  $\mu$  and there is only one such subgroup, namely, the subgroup  $\mathcal{H}$  generated by  $\tau$  and  $\eta$ . Any quantity in  $K(w)$  is unmoved by  $\eta$ , so a root in  $K(w)$  is necessarily unmoved by  $\tau$ . Conversely, any quantity in  $K(w)$  that is unmoved by  $\tau$  is a root of an irreducible polynomial of degree  $\mu$ , unless it is constant. In short, the elements of  $K(w)$  that are roots of irreducible polynomials of degree  $\mu$  are the nonconstant elements that are unmoved by the automorphism  $\tau$  of  $K(w)$ .

**Proposition 8.1.** *Let  $G(x)$  be an irreducible polynomial that is constructed as in Theorem 2.1, and let the notation be as in Section 7. If  $\kappa$  is defined by the equation  $\kappa\nu = \mu - 1$  and if  $\gamma$  is a primitive root mod  $\mu$  for which  $\delta = \gamma^\kappa$ , then a quantity in  $K(w)$  that is invariant under  $\tau$  can be written in one and only one way in the form*

$$(8.1) \quad c + \sum_{i=0}^{\kappa-1} \sum_{j=1}^{\nu} F_i(r_j) w_j^{\gamma^{-i}},$$

where, for each  $i$ ,  $F_i(x)$  is a polynomial with coefficients in  $K$  whose degree is less than  $\nu$ .

When  $\nu = \mu - 1$ , (8.1) is  $c + F(r_1)w_1 + F(r_2)w_2 + \cdots + F(r_{\mu-1})w_{\mu-1}$ , which is essentially the formula given by Kronecker<sup>15</sup> when he says that (2.1) describes the most general quantities whose  $\mu$ th roots  $s_i$  have the property that  $c + s_1 + s_2 + \cdots + s_{\mu-1}$  is a root of an irreducible equation of degree  $\mu$ . A quantity of the form (8.1) is a root of an irreducible polynomial of degree  $\mu$  (solvable, of course) unless it is constant, or, what is the same, unless the  $F_i(x)$  are all zero.

<sup>15</sup>I confess that I am unable to follow Heinrich Weber's treatment of the theorem in [18, §193 and §194], but the fact that he does not seem to modify Kronecker's formula in the case  $\nu < \mu - 1$  makes me doubt the validity of his formulation. Fricke's revision [8] of it is somewhat clearer, but he says, "*Es muß dahin gestellt bleiben, ob einige der Zahlen  $R(\phi_i)$  verschwinden.*" I suspect that the cases in which some of the numbers  $R(\phi_i)$  vanish are those in which  $\nu < \mu - 1$ .

*Proof.* Since  $\tau$  carries  $F_i(r_j)w_j^{-i} \mapsto F_i(r_{j+1})w_{j+1}^{-i}$ , a quantity in  $K(w)$  of the form (8.1) is obviously unchanged by  $\tau$ , so what is to be shown is that a quantity unchanged by  $\tau$  can be written in the form (8.1) in just one way.

Let  $q$  be in  $K(w)$ , which is to say that  $q = \sum_{l=0}^{\mu\nu-1} a_l w^l$ , where the coefficients  $a_l$  in  $K$  are determined by  $q$ , and let  $q$  be invariant under  $\tau$ . Proposition 4.1 shows that the Galois group of  $G(x)$  over  $K$  has order  $\mu\nu\lambda$  for some  $\lambda$  and is generated by three explicit automorphisms  $\sigma$ ,  $\tau$ , and  $\eta$  of the splitting field  $\Omega$  of  $G(x)$  over  $K$ . Assume without loss of generality that  $\sigma(w) = \alpha^{-1}w$  ( $\sigma$  can be replaced by any power of  $\sigma$  provided the exponent is not  $0 \pmod{\mu}$ ), define  $q_i$  to be  $\sigma^i(q)$  for all  $i$ , and define  $s_i = \sum_{k=1}^{\mu} \alpha^k q_{k\gamma^i}$ .

The fact that  $\sum_{k=1}^{\mu} \alpha^{kl}$  is  $\mu$  when  $l \equiv 0 \pmod{\mu}$  and zero otherwise implies that

$$s_i = \sum_{k=1}^{\mu} \alpha^k \sigma^{k\gamma^i} \left( \sum_{l=0}^{\mu\nu-1} a_l w^l \right) = \sum_{k=1}^{\mu} \sum_{l=0}^{\mu\nu-1} a_l \alpha^{k-lk\gamma^i} w^l = \mu \sum_{l\gamma^i \equiv 1 \pmod{\mu}} a_l w^l,$$

where  $0 \leq l < \mu\nu$ . In other words,  $s_i$  is  $\mu$  times the sum of  $a_l w^l$  over  $\nu$  values of  $l$ , namely, those between 0 and  $\mu\nu$  that are congruent to  $\gamma^{-i} \pmod{\mu}$ . In particular,  $s_i$  is in  $K(w)$ . Moreover,  $s_i/w^{\gamma^{-i}}$  is a sum of terms  $\mu a_l w^{l-\gamma^{-i}}$  in which  $w$  occurs with an exponent that is a multiple of  $\mu$ . Therefore,  $s_i = C_i(r_1)w^{\gamma^{-i}}$ , where  $C_i(x)$  is a polynomial of degree less than  $\nu$  with coefficients in  $K$ . When  $\tau$  is applied  $j-1$  times to this equation, one finds

$$s_{i+(j-1)\kappa} = C_i(r_j)w_j^{\gamma^{-i}}$$

when  $w$  is identified with  $w_1$ .

When  $s_{\mu-1}$  is written as  $s_0$  in  $q = \frac{1}{\mu}(p_0 + s_1 + s_2 + \dots + s_{\mu-1})$  one finds  $q = \frac{1}{\mu}(p_0 + (s_0 + s_{\kappa} + \dots + s_{(\nu-1)\kappa}) + \dots + (s_{\kappa-1} + s_{2\kappa-1} + \dots + s_{\nu\kappa-1})) = \frac{p_0}{\mu} + \frac{1}{\mu} \sum_{j=1}^{\nu} C_0(r_j)w_j^{\gamma^0} + \dots + \frac{1}{\mu} \sum_{j=1}^{\nu} C_{\kappa-1}(r_j)w_j^{\gamma^{-(\kappa-1)}}$ , which expresses  $q$  in the form (8.1) when  $c = \frac{p_0}{\mu} = \frac{q_1+q_2+\dots+q_{\mu-1}}{\mu}$  and  $F_i(x) = \frac{1}{\mu}C_i(x)$ .

This representation is unique, because the formula  $s_i/w^{\gamma^{-i}} = C_i(r_1) = \mu F_i(r_1)$  shows that  $q$ , which determines the  $s_i$ , determines the polynomials  $F_i(x)$ .  $\square$

### 9. THE KRONECKER-WEBER THEOREM AND KRONECKER'S JUGENDTRAUM

Most number theorists know what Kronecker dreamt of proving in his youth—his “*liebsten Jugendtraum*,” as he put it in a letter [13] to Richard Dedekind in 1880. He told Dedekind he had hoped to show that the transformation equations of elliptic functions with singular moduli could be used to construct the abelian extensions of quadratic number fields in the same way that the equations of cyclotomy can be used, according to the Kronecker-Weber theorem, to construct abelian extensions of the rational numbers.

Note, by the way, that Kronecker wrote this in 1880, taking it as known that all abelian extensions of the rationals are cyclotomic, six years before Weber published his proof [17]. The certainty with which he asserts this “Kronecker-Weber theorem” reinforces the clear statement of it as a “result” in his 1853 paper. Interestingly, the only hint of a proof in the entire 1853 paper is his brief treatment of the Kronecker-Weber theorem in the case of prime degree. He says his explanation will indicate his method for the general case, but, for this reader at least, his explanation leaves many questions unanswered. The crucial element is a wonderful formula from

Kummer's study of cyclotomy which is closely related to the question at hand, but the exact way in which Kronecker intends to use it is not altogether clear even if one understands his formula III (i.e., (2.1)) and its relation to Kummer's formula.

At the end of the 1853 paper he mentions not only the Kronecker-Weber theorem but also the even more ambitious *Jugendtraum*. He states outright that abelian extensions of the Gaussian integers are related to the equations for the division of the lemniscate in the same way that abelian extensions of the rationals are related to the equations for the division of the circle and even says "one can" generalize the result to abelian extensions of fields composed of "*bestimmte algebraische Zahlenirrationalitäten*," which is less restrained than the phrase "*Gleichungen mit Quadratwurzeln rationaler Zahlen*" that he used in the letter to Dedekind.

The unraveling of the exact meaning and validity of these intimations Kronecker made about abelian extensions of number fields is at the core of Hilbert's 12th problem, on which much work has been done. Perhaps the elucidation of Kronecker's formula III by Theorem 2.1 and Proposition 8.1 will make further progress on it possible.

#### ABOUT THE AUTHOR

Harold M. Edwards is Professor Emeritus at New York University. He has received the Whiteman and Steele Prizes of the AMS and is the author of eight books: *Advanced Calculus*, *Riemann's Zeta Function*, *Fermat's Last Theorem*, *Galois Theory*, *Divisor Theory*, *Linear Algebra*, *Essays in Constructive Mathematics*, and *Higher Arithmetic*.

#### REFERENCES

1. N. H. Abel, *Extraits de quelques lettres à Crelle*, Oeuvres, vol. 2, p. 266 (of the 1881 edition).
2. D. A. Cox, *Galois Theory*, Wiley, 2004. MR2119052 (2006a:12001)
3. H. M. Edwards, *On the Kronecker Nachlass*, *Historia Mathematica*, **5** (1978), 419–426. MR511178 (81c:01032)
4. H. M. Edwards, *Galois Theory*, Springer, New York, 1984. MR743418 (87i:12002)
5. H. M. Edwards, *An Appreciation of Kronecker*, *Mathematical Intelligencer*, **9** (1987), 28–35. MR869537 (88h:01026)
6. H. M. Edwards, *Essays in Constructive Mathematics*, Springer, New York, 2005. MR2104015 (2005h:00010)
7. H. M. Edwards, "Kronecker's Fundamental Theorem of General Arithmetic" in *Episodes in the History of Modern Algebra (1800–1950)*, Gray and Parshall, eds., AMS/LMS, 2007, pp. 107–116. MR2353493
8. R. Fricke, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1924.
9. É. Galois, "Mémoire sur les conditions de résolubilité des équations par radicaux" in *Œuvres et Mémoires mathématiques*, Paris, 1976, pp. 43–101 (English translation in [4], pp. 101–113).
10. L. Kronecker, *Beweis, dass . . .*, *Crelle* **29** (1845), 280. *Werke*, vol. 1, pp. 3–4. MR0237286 (38:5576)
11. L. Kronecker, *Über die algebraisch auflösbaren Gleichungen*, *Monatsber. Berlin*, 1853, 365–374. *Werke*, vol. 4, 3–11. MR0237286 (38:5576)
12. L. Kronecker, *Einige Entwicklungen aus der Theorie der algebraischen Gleichungen*, *Monatsber. Berlin*, 1879, 205–229, *Werke*, vol. 4, 78–96. MR0237286 (38:5576)
13. L. Kronecker, *Auszug aus einem Briefe von L. Kronecker an R. Dedekind*, *Werke*, vol. 5, 453–457. MR0237286 (38:5576)
14. E. Netto, *Theory of Substitutions* (a translation, with extensive revisions by the author, of an 1880 work *Substitutionentheorie*), Wahr, Ann Arbor, 1892. (Chelsea reprint, 1964).
15. E. Netto, *Vorlesungen über Algebra*, Teubner, Leipzig, 1900.
16. B. Petri and N. Schappacher, *From Abel to Kronecker* in *The Legacy of Niels Henrik Abel*, Laudal and Piene, eds., Springer, 2004, pp. 227–266. MR2077575 (2005e:12001)

17. H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Mathematica, **8** (1886), 193–263. MR1554698
18. H. Weber, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1895 (Reprint, AMS/Chelsea).
19. A. Wiman, *Über die metacyklischen Gleichungen von Primzahlgrad*, Acta Mathematica, vol. 27 (1903), 163–175. MR1554979

DEPARTMENT OF MATHEMATICS, NEW YORK UNIVERSITY, 251 MERCER ST., NEW YORK, NEW YORK 10012