# ROOTS OF SOLVABLE POLYNOMIALS OF PRIME DEGREE

HAROLD M. EDWARDS

Abstract. An explicit formula for the most general root of a solvable polynomial of prime degree is stated and proved. Such a root can be expressed rationally in terms of a single compound radical determined by the roots of a cyclic polynomial whose degree divides $\mu - 1$, where $\mu$ is the prime. The study of such formulas was initiated by a formula of Abel for roots of quintic polynomials that are solvable, and was carried forward by Kronecker and a few others, but seems to have lain dormant since 1924. A formula equivalent to the one given here is contained in a paper [14] of Anders Wiman in 1903, but it seems to have been forgotten.

## 1. Introduction

Shortly after Niels Henrik Abel's death in 1829, A. J. Crelle published an excerpt [1] from a letter he had received from Abel in 1826, in which Abel had stated, without explanation, a formula that he claimed represented the most general root of a solvable quintic with rational coefficients. That is, the formula described a quantity in an extension of the field of rational numbers, constructed using radicals, that not only was a root of an irreducible polynomial of degree 5 with rational coefficients, but also contained enough parameters—so Abel claimed—that it could represent, when the parameters were correctly chosen, a root of *any* given irreducible polynomial of degree 5 with rational coefficients, provided, of course, that the polynomial was one whose roots were expressible by radicals.

Abel's amazing and baffling assertion probably inspired[1] Leopold Kronecker's similarly amazing paper [10] of 1853, in which he generalized Abel's formula to the case of roots of solvable polynomials of any prime degree. Kronecker's formula accomplished in the general case somewhat less than Abel's formula had accomplished in the quintic case, because it depended upon being able to construct the roots of the most general cyclic polynomial of any given degree, whereas Abel *provided* the roots that were needed in the quintic case (see Appendix 1 below).[2] Kronecker, like Abel, did not prove his assertions.

The author thanks Thierry Coquand and David Cox for valuable comments on earlier versions of this paper.

[1]The link between [1] and Kronecker's work is obscured by the fact that Volume 4 of Kronecker's *Werke* directs the reader to the republication of [1] in the 1881 edition of Abel's *Oeuvres,* and this edition does not cite the original 1830 publication. Kronecker mentions [1] explicitly on the first page of [10], and later in the paper gives a specific reference—to the 1839 edition of Abel's *Oeuvres,* not to the original publication which he surely knew—but he says it was *wenig beachtete* (little noticed).

[2]In [10], Kronecker does make some remarks about this secondary problem of constructing roots of cyclic polynomials, as is mentioned in Section 5 below. The genesis of class field theory lies in these remarks, but that is another story.

The formulas of Abel and Kronecker in fact are valid only in what might be considered to be the generic case, the one in which $\nu = \mu - 1$ in the notation used below.[3] Heinrich Weber's *Lehrbuch der Algebra* ostensibly gives a formula that is valid generally, but in fact it only covers this generic case (see Section 6 below). The first published formula that was valid in all cases was that of Anders Wiman in 1903 [14].

After Robert Fricke's revision [7] of Weber's *Lehrbuch* in 1924, the only investigation of explicit formulas for roots of solvable polynomials of prime degree that I am aware of is my own paper [5] in which I reached a formula equivalent to Wiman's, although I didn't realize it at the time. I had found Wiman's proof too difficult to follow, and only recently, while revising and simplifying my own proof and reviewing Wiman's, did I realize that the two formulas agree. The exposition in the present paper shortens and clarifies the one given in [5] and corrects an error in that paper (see Appendix 2 below).

It probably needs to be emphasized that Abel's formula is not "a solution of solvable quintics" in the sense that the quadratic formula is a solution of quadratics, because it does not give an algorithm for going from a given solvable quintic to an expression of its roots in terms of radicals. Instead, it is an expression involving radicals and parameters that has the property that, given any solvable quintic, it is possible to choose values for the parameters in such a way that the quantity is a root of the given quintic. The proof that the formula has this property does *not* provide an algorithm for finding the requisite values of the parameters. (See Appendix 3 below.)

The formula developed here does the same for solvable polynomials of any odd prime degree $\mu$. Section 2 presents an algorithm for constructing solvable *extensions* of prime degree $\mu$ of a given ground field $K$—that is, extensions of $K$ of degree $\mu$ in which all quantities can be expressed in terms of radicals. Section 3 proves that every irreducible solvable polynomial of degree $\mu$ has a root in some extension constructed in this way. Section 4 then gives a formula (4.1) for the most general quantity in a field constructed by the algorithm, thereby describing the most general quantity expressible in terms of radicals that is a root of an irreducible polynomial of degree $\mu$. The final two sections explain the relation of formula (4.1) to the formulas of Abel and Kronecker.

## 2. A Construction of Solvable Extensions of Prime Degree

Let $K$ be a field that is either the rational field $\mathbf{Q}$ or a field obtained from $\mathbf{Q}$ by a finite number of adjunctions, either algebraic or transcendental.[4] A solvable extension of $K$ of prime degree can be constructed using the following algorithm.

---

[3] In a later paper, Kronecker gave formulas (see (III) and (IV) in [11]) that closely resemble formula (4.1) below, which shows, in my opinion, that he understood the general case, at least by 1856. In all likelihood Abel would also have understood the general case.

[4] This is, I believe, the type of field Kronecker posited, although he did not of course use the term "field" and there is some ambiguity in his description. At first he just refers to "quantities" $A$, $B$, $C$, ... that may occur in the coefficients of the polynomial. He then says that "special values" are not to be substituted, which would seem to indicate that he intends for them to be transcendental quantities, but then, in the next to last paragraph of the paper, he considers the case in which $A$, $B$, $C$, ... are integers.

**Theorem 2.1.** *Given a field $K$ of the type just described and a prime $\mu > 2$, choose a factor $\nu$ of $\mu - 1$, an irreducible cyclic[5] polynomial $f(x)$ of degree $\nu$ with coefficients in $K$, and a positive integer $\delta$ whose order mod $\mu$ is $\nu$. Let $r_1$, $r_2$, ..., $r_\nu$ be the roots of $f(x)$, in one of their cyclic orders, and let $K \subset K(r) \subset K(w)$ be the extension of $K$ obtained by first adjoining one root $r$ (and therefore all roots) of $f(x)$ and then adjoining a $\mu$th root $w$ of $r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} r_3^{\delta^{\nu-3}} \cdots r_\nu$. Assume $K(w)$ actually extends $K(r)$—that is, assume this quantity does not already have a $\mu$th root in $K(r)$. Then $K(w)$ is an extension of $K$ of degree $\mu\nu$. It has an automorphism of order $\nu$ that extends the automorphism[6] $r_i \mapsto r_{i+1}$ of $K(r)$, and the quantities in $K(w)$ that are unmoved by that automorphism constitute an extension of $K$ of degree $\mu$, as was to be constructed.*

The cyclic polynomial $f(x)$ is *a fortiori* solvable, so $r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} r_3^{\delta^{\nu-3}} \cdots r_\nu$ is expressible by radicals. Therefore $w$ is expressible by radicals, which implies that $K(w)$ is a solvable extension of $K$, as are all of its subextensions. In particular, the subextension of degree $\mu$ constructed by the theorem is solvable.

*Proof.* Let $R_i = r_{i+1}^{\delta^{\nu-1}} r_{i+2}^{\delta^{\nu-2}} r_{i+3}^{\delta^{\nu-3}} \cdots r_{i+\nu}$. The assumption that $R_0$ is not a $\mu$th power in $K(r)$ implies that $R_i$ has $\nu$ distinct values, as the following argument shows.[7] If $\nu = 1$ there is nothing to prove. If $\nu > 1$ and if $R_0 = R_\kappa$ for some $\kappa$ in the range $0 < \kappa < \nu$, then, with $a = r_1^{\delta^{\kappa-1}} r_2^{\delta^{\kappa-2}} \cdots r_\kappa$ and $b = r_{\kappa+1}^{\delta^{\nu-\kappa-1}} r_{\kappa+2}^{\delta^{\nu-\kappa-2}} \cdots r_\nu$, one finds $R_0 = a^{\delta^{\nu-\kappa}} b$ and $R_\kappa = b^{\delta^\kappa} a$. If $R_0$ and $R_\kappa$ were equal, one would have $a^{\delta^{\nu-\kappa}} b = b^{\delta^\kappa} a$, from which $a^{\delta^{\nu-\kappa}-1} = b^{\delta^\kappa - 1}$ would follow. Then $R_0^{\delta^\kappa - 1}$ would be $a^{\delta^{\nu-\kappa}(\delta^\kappa-1)} b^{\delta^\kappa-1} = a^{\delta^\nu - \delta^{\nu-\kappa}} \cdot a^{\delta^{\nu-\kappa}-1} = a^{\delta^\nu - 1}$. Since $\delta^\kappa - 1$ is relatively prime to $\mu$ (because $\kappa$ is less than the order $\nu$ of $\delta$ mod $\mu$), there would be integers $s$ and $t$ for which $(\delta^\kappa - 1)s = t\mu + 1$ and it would follow that $R_0^{t\mu+1} = R_0^{(\delta^\kappa-1)s} = a^{(\delta^\nu-1)s}$, which is impossible, because the right side is a $\mu$th power while the left side is $R_0$ times a nonzero $\mu$th power, contrary to the assumption that $R_0$ is not a $\mu$th power.

Therefore, the identity is the only element of the cyclic Galois group of $f(x)$ that leaves the $R_i$ fixed, which means that *adjoining any one $R_i$ to $K$ gives all of $K(r)$.*

By a basic lemma of Galois theory,[8] the polynomial $x^\mu - R_0$ is irreducible over $K(r)$, so $K(w)$ is an extension of $K(r)$ of degree $\mu$ and therefore is an extension of $K$ of degree $\mu\nu$.

Let $m$ be the integer $\frac{\delta^\nu - 1}{\mu}$. The $\mu$th power of $\frac{w^\delta}{r_1^m}$ is $\frac{R_0^\delta}{r_1^{\delta^\nu - 1}} = \frac{r_1 R_0^\delta}{r_1^{\delta^\nu}} = R_1$, so $w_1 = \frac{w^\delta}{r_1^m}$ is a root of

$$G(x) = \prod_{i=0}^{\nu-1} (x^\mu - R_i),$$

the same polynomial with coefficients in $K$ of which $w$ is a root. This polynomial is irreducible over $K$ because $K \subset K(w)$ is an extension of degree $\mu\nu$, so the rule $w \mapsto w_1$ determines an automorphism of $K(w)$ that carries $R_0 \mapsto R_1$ and therefore carries $r_i \mapsto r_{i+1}$ for each $i$. Iteration of this automorphism carries $w_1 \mapsto w_2 \mapsto$

[5] A cyclic polynomial is one whose Galois group is cyclic. In particular, adjunction of one root of an irreducible cyclic polynomial constructs a splitting field.

[6] Subscripts on $r$ are to be treated as integers mod $\nu$. Thus, this automorphism carries $r_\nu \mapsto r_1$.

[7] I am indebted to Thierry Coquand of the University of Gothenburg for this argument.

[8] If a polynomial $x^\mu - a$ is reducible over a field containing $a$, then it must have a linear factor over that field. For example, see [3], Proposition 4.2.6.

$\cdots \mapsto w_\nu$, where $w_i$ is a $\mu$th root of $R_i$ for $i = 1, 2, \ldots, \nu$ respectively. Specifically, $w_2 = \left(\frac{w^\delta}{r_1^m}\right)^\delta \cdot \frac{1}{r_2^m} = \frac{w^{\delta^2}}{r_1^{m\delta} r_2^m}$, $w_3 = \frac{w^{\delta^3}}{r_1^{m\delta^2} r_2^{m\delta} r_3^m}$, $\ldots$, $w_\nu = \frac{w^{\delta^\nu}}{(r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots\ r_\nu)^m} = \frac{w^{\delta^\nu}}{w^{\mu m}} = w$, which shows that the $\nu$th iterate of the automorphism is the identity. The formula $w_i^\mu = R_i$ shows that the $\nu$ images $w_1, w_2, \ldots, w_\nu = w$ are distinct, so the automorphism has order $\nu$.

It remains to show that the subfield of $K(w)$ consisting of quantities that are unmoved by this automorphism has degree $\mu$ over $K$. To this end, let a primitive $\mu$th root of unity $\alpha$ be adjoined, if necessary, to $K(w)$ to construct a splitting field $\Omega = K(w, \alpha)$ of $G(x)$ over $K$. (Each factor of $G(x) = \prod_{i=0}^{\nu-1}(x^\mu - R_i)$ has a root $w_i$ in $K(w)$, so $G(x)$ splits into linear factors after $\alpha$ is adjoined.)

An element of the Galois group of $G(x)$ must carry $w$ to one of the roots of $G(x)$ in $\Omega$, say $w \mapsto \alpha^j w_i$, and must carry $\alpha$ to some power of $\alpha$ other than 1, say $\alpha \mapsto \alpha^\epsilon$ where $\epsilon \not\equiv 0 \bmod \mu$. Such an automorphism carries $w^\mu \mapsto w_i^\mu$; thus, $R_0 \mapsto R_i$ for this $i$ and the automorphism carries $r_k \mapsto r_{k+i}$ for each $k$. As was shown above in the case $c = 0$,

$$w_{c+l} = \frac{w_c^{\delta^l}}{(r_{c+1}^{\delta^{l-1}} r_{c+2}^{\delta^{l-2}} \cdots r_{c+l})^m}$$

from which it follows that the automorphism carries $w_l \mapsto \alpha^{j\delta^l} w_{i+l}$ for all $l$. (Use the formula with $c = 0$ for $w_l$ and with $c = i$ for $w_{i+l}$, then use $w \mapsto \alpha^j w_i$ and $r_k \mapsto r_{k+i}$.) When $\alpha \mapsto \alpha^\epsilon$ as above, this gives the formula $\alpha^k w_l \mapsto \alpha^{\epsilon k} \cdot \alpha^{j\delta^l} w_{i+l} = \alpha^{\epsilon k + j\delta^l} w_{i+l}$ for the effect of an element of the Galois group of $G(x)$ on the roots of $G(x)$. (Every permutation of the roots of $G(x)$ that is effected by the Galois group must have this form, but there may well be permutations of this form that are not effected by the Galois group, because $\epsilon$ is not independent of $\alpha^j w_i$.)

In particular, the only possible images of $t = w_1 + w_2 + \cdots + w_\nu$ under the Galois group are $\alpha^{j\delta} w_{i+1} + \alpha^{j\delta^2} w_{i+2} + \cdots + \alpha^j w_{i+\nu}$. The exponent on $\alpha$ in the coefficient of any $w_k$ determines the exponent on $\alpha$ in the coefficient of all others, because for $w_{k+1}$ the exponent is $\delta$ times what it is for $w_k$ (mod $\mu$). Therefore, the possible conjugates of $t$ under the Galois group are $t_k = \alpha^k w_1 + \alpha^{k\delta} w_2 + \alpha^{k\delta^2} + \cdots + \alpha^{k\delta^{\nu-1}} w_\nu$ for $k = 1, 2, \ldots, \mu$, so $t$ has at most $\mu$ distinct conjugates in $\Omega$.

By basic Galois theory, the polynomial $\prod_{k=1}^{\mu}(x - t_k)$ is a power of an irreducible polynomial with coefficients in $K$. Since $\mu$ is prime, then, either $t$ is a root of an irreducible polynomial of degree $\mu$ or the $t_k$ are all the same and are in $K$. The latter is impossible because $\sum_{k=1}^{\mu} \alpha^{-k} t_k = \mu w_1$ is not zero, as it would be if $t = t_k$ for all $k$, because then it would be $t \sum_{k=1}^{\mu} \alpha^{-k} = 0$. Therefore, adjunction of $t$ gives a subextension $K \subset K(t) \subset K(w)$ of degree $\mu$. As the above formula for the action of the Galois group on the roots of $G(x)$ shows, the elements of the Galois group that leave $t$ unmoved are precisely those that permute the $w$'s cyclically, and the proof of the theorem is complete. □

## 3. The Construction Finds All Solvable Extensions of Prime Degree

**Theorem 3.1.** *Any solvable irreducible polynomial $g(x)$ of prime degree $\mu$ with coefficients in $K$ has a root in the extension of $K$ constructed by the method of Theorem 2.1 when $\nu$, $f(x)$, and $\delta$ are chosen suitably.*

*Proof.* As was proved by Galois himself [8], the Galois group of $g(x)$, when it is regarded as a group of permutations of the roots $q_k$ of $g(x)$, is a group generated by

two permutations $q_k \mapsto q_{k+1}$ and $q_k \mapsto q_{\zeta k}$ for some integer $\zeta \not\equiv 0 \bmod \mu$, when the roots are suitably ordered (and when the subscripts on the roots are interpreted as integers mod $\mu$).

Let $\Omega$ be the field obtained by adjoining a $\mu$th root of unity $\alpha \neq 1$ to the splitting field of $g(x)$, and let $\mathcal{G}$ be the Galois group of $\Omega$ over $K$. Since $\Omega$ is a normal extension of the splitting field of $g(x)$ (adjoining one $\mu$th root of unity $\alpha \neq 1$ adjoins all because all are powers of any one), the Galois group of $g(x)$ is a quotient group of $\mathcal{G}$. In particular, the order of $\mathcal{G}$ is divisible by $\mu$, so $\mathcal{G}$ must contain an element of order $\mu$, call it $\sigma$. Since $\sigma$ partitions the $\mu - 1$ powers of $\alpha$ other than 1 into orbits, each of whose lengths divides the prime $\mu$, these orbits must all have length 1, which is to say that $\sigma(\alpha) = \alpha$. If $\sigma$ left any root of $g(x)$ fixed, the same argument would imply that it left all roots of $g(x)$ fixed, which would imply that $\sigma$ was the identity, contrary to the assumption that it has order $\mu$. Therefore, since $\sigma$ must act on the roots without leaving any fixed, and since it must effect a permutation of the form $q_k \mapsto q_{ak+b}$, it must permute the roots of $g(x)$ according to the formula $q_k \mapsto q_{k+b}$ for some integer $b \not\equiv 0 \bmod \mu$. Since each such permutation is a power of any other, $\sigma$ can be assumed without loss of generality to carry $q_k \mapsto q_{k+1}$ and $\alpha \mapsto \alpha$, which determines its action on $\Omega$.

Consider the quantities $s_i = \sum_{k=1}^{\mu} \alpha^k q_{ki}$ in $\Omega$. (These are the Lagrange resolvents of $g(x)$. The fact that $q_k$ is defined for all integers $k$ implies that $s_i$ is defined for all integers $i$. It depends only on the class of $i \bmod \mu$ and is zero when $i \equiv 0 \bmod \mu$. In what follows, $i$ will be assumed to be nonzero mod $\mu$.) The effect of $\sigma$ on $s_i$ is given by $\sigma(s_i) = \sum_{k=1}^{\mu} \alpha^k q_{ki+1} = \sum_{l=1}^{\mu} \alpha^{i^{-1}(l-1)} q_l = \alpha^{-i^{-1}} \sum_{l=1}^{\mu} \alpha^{i^{-1}l} q_l = \alpha^{-i^{-1}} s_i$ where $i^{-1}$ represents an integer that is inverse to $i \bmod \mu$. Given an element $\theta$ of $\mathcal{G}$, there is a unique $k \bmod \mu$ for which $\theta = \sigma^k h$ where $h$ leaves $q_\mu$ unmoved, namely, the $k$ for which $\theta(q_\mu) = q_k$. (Composition is here written from right to left. Of course $\theta$ must carry a root of $g(x)$ to a root of $g(x)$.) In particular, the subgroup $\mathcal{H}$ of elements of $\mathcal{G}$ that leave $q_\mu$ unchanged has index $\mu$. Any $h$ in $\mathcal{H}$ carries $\alpha \mapsto \alpha^u$ and $q_k \mapsto q_{kv}$ for some integers $u$ and $v$, neither of which is 0 mod $\mu$, so it carries $s_i \mapsto \sum_{k=1}^{\mu} \alpha^{ku} q_{kvi} = \sum_{l=1}^{\mu} \alpha^l q_{lu^{-1}vi} = s_{u^{-1}vi}$, where $u^{-1}$ is an integer that is inverse to $u \bmod \mu$. Assigning to each $h$ in $\mathcal{H}$ the corresponding integer $u^{-1}v$ in the multiplicative group of nonzero integers mod $\mu$ gives a homomorphism from $\mathcal{H}$ to a cyclic group of order $\mu - 1$. The image of this homomorphism is of course a cyclic group of order $\nu$ for some divisor $\nu$ of $\mu - 1$. Let $\delta$ be an integer whose order mod $\mu$ is $\nu$. Then the orbit of $s_i$ under the action of $\mathcal{H}$ contains precisely those $s_k$ for which $k = i\delta^j$, where $j = 1, 2, \ldots, \nu$. In other words, the permutations of the $s_i$ effected by $\mathcal{H}$ are those of the form $s_i \mapsto s_{i\delta^j}$.

The binomial theorem implies that if $\delta^\nu \equiv 1 \bmod \mu^2$ then $(\delta + \mu)^\nu \not\equiv 1 \bmod \mu^2$, so one can assume without loss of generality that $\delta^\nu \not\equiv 1 \bmod \mu^2$.

At least one of the quantities $s_i$ must be nonzero, because when $c$ is defined to be $q_1 + q_2 + \cdots + q_\mu$, the formula $\mu q_\mu = c + s_1 + s_2 + \cdots + s_{\mu-1}$ holds, and the left side is not in $K$ (because $g(x)$ is irreducible over $K$) but the right side would be in $K$ if the $s_i$ were all zero ($c$ is a symmetric function of the roots of $g(x)$). Choose an integer $\iota$ for which $s_\iota \neq 0$.

When $\nu = 1$, let $w = s_\iota$. An element $\sigma^k h$ of $\mathcal{G}$ that leaves $s_\iota$ fixed must have $k \equiv 0 \bmod \mu$ because $h$ leaves $s_\iota \neq 0$ fixed (because $\nu = 1$) and $\sigma$ multiplies it by $\alpha^{-\iota^{-1}} \neq 1$. Such an element leaves $s_i$ fixed for every $i$, so it leaves $q_\mu = \frac{1}{\mu}(c + s_1 + s_2 + \cdots + s_{\mu-1})$ fixed. Therefore, $K(s_\iota)$ contains a root of $g(x)$. On the

other hand, $s_\iota^\mu$ is fixed under all of $\mathcal{G}$, which means that $K(s_\iota)$ adjoins a $\mu$th root to $K$, which is the construction of Theorem 2.1 in the case $\nu = 1$.

When $\nu > 1$, let $\nu$ quantities in $\Omega$ be defined by

$$r_j = \frac{s_{\iota\delta^{\nu-j}}}{s^\delta_{\iota\delta^{\nu-j+1}}}. \tag{3.1}$$

(Note that the denominators are nonzero, because they are the $\delta$th powers of the quantities in the orbit of $s_\iota$ under $\mathcal{H}$.) Since $\sigma$ multiplies the numerator of $r_j$ by $\alpha^{-\iota^{-1}\delta^{-\nu+j}}$ and multiplies the denominator by the same factor $(\alpha^{-\iota^{-1}\delta^{-\nu+j-1}})^\delta$, $\sigma(r_j) = r_j$ for each $j$. Since elements of $\mathcal{H}$ permute the $s_{\iota\delta^k}$ cyclically, they also permute the $r_j$ cyclically, and since $\sigma$ and $\mathcal{H}$ generate $\mathcal{G}$, it follows that $\mathcal{G}$ effects only cyclic permutations of the $r_j$ and therefore that *the $r_j$ are the roots of a cyclic polynomial of degree $\nu$ with coefficients in $K$,* call it $f(x)$. That $f(x)$ is irreducible will be shown below.

When the $r_j$ are defined in this way, the quantity $R_0 = r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} \cdots\ r_{\nu-1}^\delta r_\nu$ in $\Omega$ is a product in which the numerator of each term is cancelled by the denominator of the following term, leaving just the denominator of $r_1^{\delta^{\nu-1}}$ and the numerator of $r_\nu$, which is to say $R_0 = s_\iota / s_\iota^{\delta^\nu}$, so $R_0$ is the $\mu$th power of $s_\iota^{-m}$, where $m = \frac{\delta^\nu - 1}{\mu}$ and where, by the choice of $\delta$, $m \not\equiv 0 \bmod \mu$.

Thus, $\Omega$ contains a $\mu$th root of $R_0$, which means that it contains a root of the polynomial $G(x) = \prod_{i=0}^{\nu-1}(x^\mu - R_i)$, where the $R_i$ are the $\nu$ conjugates $s_{\iota\delta^i}^{-\delta^\nu+1}$ of $R_0$ under $\mathcal{G}$. Since elements of $\mathcal{G}$ permute the $r_i$ cyclically, these conjugates are $R_i = r_{i+1}^{\delta^{\nu-1}} r_{i+2}^{\delta^{\nu-2}} r_{i+3}^{\delta^{\nu-3}} \cdots\ r_{i+\nu}$ for $i = 0, 1, \ldots, \nu - 1$ and $G(x)$ has coefficients in $K$. By the definition of $\delta$, $\mathcal{H}$ acts transitively on the $s_{\iota\delta^j}^{-m}$; these $\nu$ quantities are distinct, because they are nonzero and application of $\sigma$ to them multiplies them by different powers of $\alpha$, namely, it multiplies $s_{\iota\delta^j}^{-m}$ by $\alpha^{m\iota^{-1}\delta^{-j}}$ (and $m \not\equiv 0 \bmod \mu$). The elements $\sigma^k h$ of $\mathcal{G}$ then carry $s_\iota^{-m}$ to $\mu\nu$ distinct quantities in $\Omega$—namely, the quantities $\alpha^\kappa s_{\iota\delta^j}^{-m}$ where $\kappa$ is interpreted mod $\mu$ and $j$ is interpreted mod $\nu$—which means that the Galois group $\mathcal{G}$ acts transitively on the roots of $G(x)$ and that $G(x)$ is irreducible over $K$. In particular, the $\nu$ quantities $R_0, R_1, \ldots, R_{\nu-1}$ are distinct, which implies that $r_1, r_2, \ldots, r_\nu$ are distinct, so $f(x)$ is irreducible.

An element $\sigma^k h$ of $\mathcal{G}$ that leaves $w = s_\iota^{-m}$ fixed must have $k \equiv 0 \bmod \mu$ *and* must leave $s_\iota$ fixed, which means that it leaves all of the $s_i$ fixed and therefore leaves the root $q = \frac{1}{\mu}(c + s_1 + s_2 + \cdots + s_{\mu-1})$ of $g(x)$ fixed. Thus $q$ is in $K(w)$. There is an $h$ in $\mathcal{H}$ that carries $s_\iota \mapsto s_{\iota\delta}$, and the restriction of such an $h$ to $K(w) = K(s_\iota^{-m})$ is an automorphism of order $\nu$ that leaves $q$ fixed (it permutes the summands of $\frac{1}{\mu}(c + s_1 + s_2 + \cdots + s_{\mu-1})$). This automorphism permutes the $w_i = s_{\iota\delta^i}^{-m}$ cyclically, so $q$ is in the subextension of $K(w)$ constructed by Theorem 2.1 for this choice of $\nu$, $f(x)$, and $\delta$. □

## 4. The Most General Root of an Irreducible Solvable Polynomial of Prime Degree with Coefficients in $K$

Theorems 2.1 and 3.1 prove that a root of an irreducible solvable polynomial of prime degree $\mu$—which by definition can be expressed in terms of radicals—can be expressed *rationally* in terms of a *single* compound radical

$$w = \sqrt[\mu]{r_1^{\delta^{\nu-1}} r_2^{\delta^{\nu-2}} r_3^{\delta^{\nu-3}} \cdots\ r_\nu}$$

of the type constructed in Theorem 2.1. Specifically, these rational expressions can be put in the following canonical form:

**Theorem 4.1.** *Each quantity in the solvable extension of $K$ of degree $\mu$ that is constructed by Theorem 2.1 has one and only one representation in the form*

$$c + \sum_{i=0}^{\kappa-1} \sum_{j=1}^{\nu} F_i(r_j) w_j^{\gamma^i} \tag{4.1}$$

*where $\kappa = \frac{\mu-1}{\nu}$, where $c$ is in $K$, where $\gamma$ is a primitive root mod $\mu$, where the $\kappa$ polynomials $F_i(x)$ with coefficients in $K$ all have degree less than $\nu$, and where $w_1, w_2, \ldots, w_\nu, r_1, r_2, \ldots,$ and $r_\nu$ can all be expressed rationally in terms of any one $w_j$.*

**Corollary 4.2.** *The expression (4.1) describes a quantity in $K(w)$ that is unchanged by $w_k \mapsto w_{k+1}$ because this cyclic permutation of the $w$'s permutes the terms of each sum over $j$ in (4.1) cyclically, so the quantity it describes generates a subextension of $K(w)$ whose degree divides $\mu$; therefore, unless the quantity is in $K$, it is a root of an irreducible polynomial of degree $\mu$ with coefficients in $K$. Conversely, any quantity that is expressible in terms of radicals and is a root of an irreducible polynomial of degree $\mu$ with coefficients in $K$ can be expressed in this form, as follows from Theorems 3.1 and 4.1. In what might be called the generic case, when $\nu = \mu - 1$, (4.1) becomes*

$$c + F(r_1)w_1 + F(r_2)w_2 + \cdots + F(r_{\mu-1})w_{\mu-1},$$

*which is the form given by Abel (in the case $\mu = 5$) and Kronecker.*

*Proof.* The uniqueness of an expression of such a quantity in the form (4.1) follows from existence, because (4.1) contains $1 + \kappa\nu = \mu$ constants and the extension constructed in Theorem 2.1 is a vector space of dimension $\mu$ over $K$.

Let $q$ be in $K(w)$, say $q = \sum_{i=0}^{\mu-1} a_i w^i$, and assume it is in the subextension of Theorem 2.1, which is to say that it is unchanged by the automorphism of $K(w)$ that carries $w_k \mapsto w_{k+1}$. Then $q = \frac{1}{\nu} \cdot \sum_{l=1}^{\nu} \sum_{i=0}^{\mu-1} a_i w_l^i$. Since a sum of quantities of the form (4.1) has the form (4.1), it will suffice to show that each $\frac{a_i}{\nu} \cdot \sum_{l=1}^{\nu} w_l^i$ has the form (4.1). Since $w_i^\mu$ is rational in $r_j$ for any $j$, it will suffice to prove that $\sum_{l=1}^{\nu} F(r_l) w_l^k$ can be put in the form (4.1) for every $k$ in the range $0 \le k < \mu$ and for every polynomial $F(x)$ of degree less than $\nu$ with coefficients in $K$. Because, as was shown in Section 2, $w_{l+1} = \frac{w_{l+1}^\delta}{r_{l+1}^m}$, this sum can also be written in the form $\sum_{l=1}^{\nu} F(r_{l+1}) \frac{w_l^{\delta k}}{r_{l+1}^m}$, which is of the form $\sum_{l=1}^{\nu} F_1(r_l) w_l^{\delta k}$, where $F_1(x)$ has degree less than $\nu$ and coefficients in $K$. (Adjoining one $r$ adjoins all.) Moreover, the exponent $\delta k$ can be replaced by the smallest positive integer congruent to it mod $\mu$. Therefore, if $\sum_{l=1}^{\nu} F(r_l) w_l^k$ can be put in the desired form for one value of $k$ in the range $0 \le k < \mu$, it can be put in the desired form for any value of $k$ in that range that is congruent to $k\delta^j$ mod $\mu$ for any positive integer $j$. The theorem then follows, because every $k$ is congruent mod $\mu$ to an integer of the form $\gamma^\phi \delta^\psi$ for some $\phi$ in the range $0 \le \phi < \kappa$. □

## 5. The Formulas of Abel and Kronecker

Abel's formula [1] for the most general root of a solvable quintic with rational coefficients is (when the notation is altered to agree with the notation used above)

$$x = c + F(r_1)\sqrt[5]{r_1r_2^2r_3^4r_4^3} + F(r_2)\sqrt[5]{r_2r_3^2r_4^4r_1^3} + F(r_3)\sqrt[5]{r_3r_4^2r_1^4r_2^3} + F(r_4)\sqrt[5]{r_4r_1^2r_2^4r_3^3},$$

where $F(r_i) = K + K'r_i + K''r_{i+2} + K'''r_ir_{i+2}$ for rational numbers $K$, $K'$, $K''$, $K'''$, and where $r_1$, $r_2$, $r_3$, and $r_4$ are given by the explicit formulas (5.1) below.

The fact that the exponents under his radicals are 1, 2, 4, 3 instead of 1, 2, 4, 8 as in Theorem 4.1 can be ignored, because $\sqrt[5]{r_{i-1}^8} = r_{i-1}\sqrt[5]{r_{i-1}^3}$ and the factor $r_{i-1}$ can be incorporated in the coefficient $F(r_i)$ because adjunction of one $r$ adjoins all.

This description of the roots $x$ is weaker than Theorem 4.1 in three ways. First, it includes only the case $\nu = 4$ of Theorem 4.1. Second, it does not explain that any one of the four 5th roots in the formula determines the other three rationally (although there can be little doubt that Abel would have understood this). Finally, as Weber [13] pointed out, Abel's form of $F(r_i)$ is not general enough,[9] because 1, $r_1$, $r_3$, $r_1r_3$ do not form a basis of $\mathbf{Q}(r)$ over $\mathbf{Q}$—clearly they are not linearly independent over $\mathbf{Q}$—and therefore neither do 1, $r_2$, $r_4$, $r_2r_4$—when the $r_i$ are given by his formulas. Thus, some quantities of the form (4.1) with $\mu = 5$ and $\nu = 4$ are not expressible in Abel's form.

However, Abel's description is much stronger in that he gives an explicit formula for the most general set of four quantities $r_i$ that are the roots of a cyclic quartic, namely,

$$\begin{aligned}
r_1 &= m + n\sqrt{1+e^2} + \sqrt{h(1+e^2+\sqrt{1+e^2})} \\
r_2 &= m - n\sqrt{1+e^2} + \sqrt{h(1+e^2-\sqrt{1+e^2})} \\
r_3 &= m + n\sqrt{1+e^2} - \sqrt{h(1+e^2+\sqrt{1+e^2})} \\
r_4 &= m - n\sqrt{1+e^2} - \sqrt{h(1+e^2-\sqrt{1+e^2})}
\end{aligned} \tag{5.1}$$

where $h$, $e$, $m$, and $n$ are rational numbers. The validity of these formulas is proved in Appendix 1 below, which implies that they can be used in Theorem 4.1 to give a formula for the most general root of a solvable quintic with rational coefficients in the case $\nu = 4$.

Kronecker's formula for the roots of a solvable polynomial of prime degree $\mu$ is contained in formulas (II) and (III) of [10] and they amount to the case $\nu = \mu - 1$ of Theorem 4.1. Like Abel, he does not mention the fact that the needed $\mu$th roots are determined rationally once one is chosen. Unlike Abel, he emphasizes that the formula not only represents *all* roots of solvable polynomials of degree $\mu$ but also represents *only* such roots. Also unlike Abel, he describes (in his formula (IV)) the remaining $\mu - 1$ conjugate roots using different $\mu$th roots $\alpha^j w$ of $w^\mu$.

As for the determination of the quantities $r_i$ that are needed by the formula—the roots of irreducible cyclic polynomials of (not necessarily prime) degree $\nu$—Kronecker states that his methods have enabled him to give a complete solution

[9] I find this lapse very puzzling. How could Abel have made the astonishing discovery of the general formula, but then given this inadequate formula for $F(r_i)$ instead of the simple formula $K + K'r_i + K''r_i^2 + K'''r_i^3$? Was there perhaps a mistake in the transcription?

(*... Methode, die ich in allen anderen Fällen mit Erfolg angewendet habe ...*) except in cases in which $\nu$ is divisible by 8, but he only hints at what those methods might be, saying that his communication is only a preliminary one (*dieser vorläufigen Mittheilung*), but as far as I know he never did divulge his methods.

## 6. Cases in Which $\nu < \mu - 1$

Both Abel and Kronecker seem to ignore cases in which $\nu < \mu - 1$. For example, there seems to be no way to use the formula they both give, namely, $x = c + F(r_1)w_1 + F(r_2)w_2 + F(r_3)w_3 + F(r_4)w_4$, to represent the quantities given by (4.1) in the case $K = \mathbf{Q}$, $\mu = 5$, $\nu = 1$, $r_1 = 2$, $\delta = 2$, which are simply the quantities $c_0 + c_1\sqrt[5]{2} + c_2(\sqrt[5]{2})^2 + c_3(\sqrt[5]{2})^4 + c_4(\sqrt[5]{2})^8$. The rational coefficients $c_i$ may be chosen arbitrarily, whereas in the formula of Abel and Kronecker the last four terms are all determined once one is specified.

This observation also causes me to doubt the formula Weber gives in his *Lehrbuch der Algebra* [13], §194, which is essentially identical to Kronecker's, but Weber seems to assert, more strongly than Abel and Kronecker did, that it applies even when $\nu < \mu - 1$, because he first claims to prove it with the additional assumptions that the Lagrange resolvents (the $s_i$ above) are all nonzero and the roots of the cyclic equation of degree $\mu - 1$ (the $r_i$ above) are distinct and then eliminates these assumptions. However, as was shown above, if only the case $\nu = \mu - 1$ is being considered, then the Lagrange resolvents are all conjugate in $\Omega$, which means they are necessarily all nonzero because at least one $s_\iota$ must be nonzero, and the $r_i$ are necessarily distinct. That is, these extra conditions that are removed are in fact automatically fulfilled for roots of equations for which $\nu = \mu - 1$, so the extra work Weber is doing would be justified only if he means to treat cases in which $\nu < \mu - 1$.

My doubts about Weber's formula stem not only from the fact that I find his proof impossible to follow and the fact that the formula does not seem to describe the most general nonconstant quantity in $\mathbf{Q}(\sqrt[5]{2})$ as above, but also from the fact that Robert Fricke seems to have disowned Weber's formula when he revised Weber's *Lehrbuch* in 1924 [7]. Instead, he proves a more limited theorem, saying that his treatment does not cover all cases and that the first exhaustive (*erschöpfend*) treatment was given by Anders Wiman in 1903 [14]. Wiman's formula (16) is essentially formula (4.1) above.

Formulas (III), (IV), and (V) of Kronecker's later paper [11] virtually imply Wiman's formula,[10] and therefore formula (4.1), except that they are stated only in the case $K = \mathbf{Q}$ and they are complicated by the fact that Kronecker incorporates in them (using what later became known as the Kronecker-Weber theorem) a formula for the most general roots of a cyclic polynomial of degree $\nu$ (which is $n$ in Kronecker's notation).

I also consider it very improbable that Abel would have completely overlooked the cases $\nu = 1$ or 2 of quintic equations, even though the formula in his 1826 letter to Crelle does seem to overlook them.

[10]Formula (III) as it appears in Kronecker's *Werke* has a typographical error; an exponent $c$ that should be outside the parentheses is inside them.

## 7. Appendix 1: Abel's Formula for the Most General Roots of a Cyclic Quartic with Rational Coefficients

**Theorem 7.1.** *If $r_1$, $r_2$, $r_3$, and $r_4$ are the roots, in cyclic order, of an irreducible cyclic polynomial of degree 4 with rational coefficients, then rational numbers $h$, $e$, $m$, and $n$ can be chosen in such a way that the $r_i$ are given by (5.1). Conversely, for any rational numbers $m$, $n$, $h$, and $e$, these formulas give, provided $eh \neq 0$, the roots of an irreducible cyclic polynomial of degree 4 with rational coefficients.*

*Proof.* Let $r_1$, $r_2$, $r_3$, and $r_4$ be the roots, in cyclic order,[11] of an irreducible cyclic polynomial of degree four in a splitting field $\mathbf{Q}(r)$ of the polynomial. Let $\phi = r_1 + r_2 - r_3 - r_4$, $\psi = r_1 - r_2 - r_3 + r_4$, and $\theta = r_1 - r_2 + r_3 - r_4$. Then $r_1 = \frac{1}{4}(\phi + \psi + \theta + C)$ where $C$ is the rational number $r_1 + r_2 + r_3 + r_4$. Since $\pm\phi$ and $\pm\psi$ constitute an orbit under the action of the Galois group (which is generated by $r_i \mapsto r_{i+1}$) either all of them are zero or none are. If all were zero, then $r_1 = \frac{1}{4}(\theta + C)$ would have order at most 2 over $\mathbf{Q}$ (the orbit of $\theta$ contains only $\pm\theta$), which is impossible. Therefore, $\phi\psi \neq 0$ and $e = \frac{\phi^2 - \psi^2}{2\phi\psi}$ is a well-defined quantity in the splitting field. The orbit of $e$ under the Galois group contains just $\pm e$, so $e^2$ is rational. Similarly, $h = \frac{\phi^2 + \psi^2}{1 + e^2}$ is a rational number because it is invariant under $r_i \mapsto r_{i+1}$. With rational numbers $e^2$ and $h$ so defined, the identity

$$\big(x^2 - (\phi + \psi)^2\big)\big(x^2 - (\phi - \psi)^2\big) = x^4 - 2h(e^2 + 1)x^2 + h^2e^2(1 + e^2)$$

is easily verified. (Note that $1 + e^2 = \big(\frac{\phi^2 + \psi^2}{2\phi\psi}\big)^2$.) The roots of this quartic are the quantities in the orbit of $\phi + \psi$ under the Galois group, so adjoining one root gives a subfield of $\mathbf{Q}(r)$. This subfield is of degree 4, because otherwise $\phi + \psi$ would be invariant under the square of a generator of the Galois group, which would mean $\phi + \psi = -\phi - \psi$ or $\phi + \psi = 0$, which would again imply $r_1 = \frac{1}{4}(\theta + C)$. Therefore, adjunction of one root $\phi + \psi$ of this quartic gives all of $\mathbf{Q}(r)$ and in particular gives an extension containing $\pm\phi$ and $\pm\psi$. Moreover, $\mathbf{Q}(r)$ contains all four roots $\pm(\phi \pm \psi)$ of $x^4 - 2h(e^2 + 1)x^2 + h^2e^2(1 + e^2)$, which, by the quadratic formula, are $\pm\sqrt{h(1 + e^2 \pm \sqrt{1 + e^2})}$. On the other hand, because $\frac{\phi^2 + \psi^2}{2\phi\psi\theta}$ is invariant under the Galois group, $\theta$ is $n \cdot \frac{\phi^2 + \psi^2}{2\phi\psi}$ for some rational $n$, so one can write $\theta = \pm n\sqrt{1 + e^2}$. Then the formulas $4r_1 = C + \theta + \phi + \psi$, $4r_2 = C - \theta + \phi - \psi$, $4r_3 = C + \theta - \phi - \psi$, and $4r_4 = C - \theta - \phi + \psi$ imply that $4r_1$, $4r_2$, $4r_3$, and $4r_4$, are represented by the formulas (5.1) as quantities in the splitting field of $x^4 - 2h(e^2 + 1)x^2 + h^2e^2(1 + e^2)$ and are in cyclic order. Since $4r_1$, $4r_2$, $4r_3$ and $4r_4$ are roots of an irreducible cyclic quartic in cyclic order if and only if $r_1$, $r_2$, $r_3$ and $r_4$ are, the first statement of the theorem follows.

Conversely, if $r_1$, $r_2$, $r_3$, and $r_4$ are given by (5.1), then $\frac{r_1 - r_3}{2} = \sqrt{h(1 + e^2 + \sqrt{1 + e^2})}$ is a root of $x^4 - 2h(1 + e^2)x^2 + h^2e^2(1 + e^2)$, call it $p$. The assumption that $eh \neq 0$ implies $p \neq 0$. Let $q = e \cdot \frac{p^2 - h(1 + e^2)}{p}$. Then $p^2q^2 = e^2 \cdot (p^2 - h(1 + e^2))^2 = e^2(p^4 - 2h(1 + e^2)p^2 + h^2(1 + e^2)^2) = e^2(-h^2e^2(1 + e^2) + h^2(1 + e^2)^2) = h^2e^2(1 + e^2)$ and $p^2 + q^2 = p^2 + \frac{h^2e^2(1 + e^2)}{p^2} = \frac{p^4 + h^2e^2(1 + e^2)}{p^2} = 2h(1 + e^2)$. Therefore, $x^4 - 2h(1 + e^2)x^2 + h^2e^2(1 + e^2) = (x^2 - p^2)(x^2 - q^2)$, which shows that the extension $\mathbf{Q}(p)$ of $\mathbf{Q}$ obtained by adjoining the one quantity $p$ contains 4 roots $\pm p$, $\pm q$ of

[11] There are eight ways of writing them in cyclic order. The two that start with $r_1$ are $r_1$, $r_2$, $r_3$, $r_4$, and $r_1$, $r_4$, $r_3$, $r_2$.

$x^4 - 2h(1+e^2)x^2 + h^2e^2(1+e^2)$. In particular, $p \mapsto q$ determines an automorphism of the field. Since this automorphism does not carry $p \mapsto -p$, it must carry $p \mapsto \pm q$. Replacing the automorphism with its inverse reverses this sign, so one can assume without loss of generality that the automorphism carries $p \mapsto q$ and $q \mapsto -p$, where, by the quadratic formula, $q = \pm\sqrt{h(1+e^2-\sqrt{1+e^2})}$. Therefore, the automorphism reverses the sign of $p^2 - q^2 = 2h\sqrt{1+e^2}$ and permutes the 4 quantities in (5.1) cyclically, as was to be shown. □

Abel's statement of the formula for the most general root of a solvable quintic (in which $\nu = 4$) is followed by an assertion that "I have found similar formulas for equations of degree 7, 11, 13, etc." Does this mean that he had found formulas like (5.1) for the most general roots of cyclic polynomials of degrees 6, 10, and 12?

## 8. Appendix 2: A Correction

The main theorems of [5] (its Theorem 2.1 and Proposition 8.1) follow from the theorems proved above. I regret to say that the proofs given in [5] are vitiated by an erroneous description (Proposition 4.1) of the group $\mathcal{G}$. Worse than this mistake was my hasty and incorrect revision of Proposition 4.1 in [6].

The descriptions of $\mathcal{G}$ in both [5] and [6] are contradicted by Example 2.2 of [5], in which $\mu = 5$, $f(x) = x^2 - 2x - 1$ and $\delta = 4$. In this case, the subgroup that leaves $w_1 + w_2$ fixed is the direct product of a group of order 2, generated by the element $\tau$ which takes $w_1 \leftrightarrow w_2$ and $\alpha \mapsto \alpha$, and a group of order 4, generated by the element $\eta$ which takes $w_i \mapsto w_i$ and $\alpha \mapsto \alpha^2$. The five quantities $w_1 + w_2$, $\alpha w_1 + \alpha^4 w_2$, $\alpha^2 w_1 + \alpha^3 w_2$, $\alpha^3 w_1 + \alpha^2 w_2$, $\alpha^4 w_1 + \alpha w_2$ are permuted cyclically by $\sigma$, which carries $w_1 \mapsto \alpha w_1$, $w_2 \mapsto \alpha^4 w_2$, and $\alpha \mapsto \alpha$. Simple computations show that neither $\tau$ nor $\eta$ commutes with $\sigma$.

## 9. Appendix 3: Solving Solvable Polynomials

As was pointed out in Section 1, formula (4.1) accomplishes something quite different from solving solvable polynomials of prime degree. However, it is not entirely unrelated. Theorem 3.1 constructs $\nu$, $f(x)$, and $\delta$ that can be used in Theorem 2.1 to construct an extension of $K$ that contains a root of a given solvable $g(x)$ of degree $\mu$. (The hardest step of the construction is the determination of the action of the Galois group of $g(x)$ on the roots of a given solvable $g(x)$.) Once that field is constructed, a root of $g(x)$ can be constructed by factoring $g(x)$ as a polynomial with coefficients in the extended field (see [4]).

## References


1. N. H. Abel, *Extrait de quelques lettres à Crelle,* Oeuvres, 1881, vol. 2, p. 266, or Oeuvres, 1839, vol. 2, p. 253. First published in German in Crelle's Journal, vol. 5 (1830) p. 336.
2. N. H. Abel, *Sur la résolution algébrique des équations,* Oeuvres, 1839 (vol. 2, pp. 185–209) or 1881 (vol. 2, pp. 217–243).
3. D. A. Cox, *Galois Theory,* Springer, New York, 1984
4. H. M. Edwards, *Essays in Constructive Mathematics*, Springer, New York, 2005
5. H. M. Edwards, *The Construction of Solvable Polynomials,* Bull. AMS, 46 (2009), 397-411
6. H. M. Edwards, *"The Construction of Solvable Polynomials," Errata,* Bull. AMS, 46 (2009), 703-704
7. R. Fricke, *Lehrbuch der Algebra,* Vieweg, Braunschweig, 1924

8. É. Galois, *Mémoire sur les conditions de résolubilité des équations par radicaux,* in *Écrits et Mémoires mathématiques,* (English translation in [12], pp. 109-135)
9. L. Gårding and C. Skau, *Neils Henrik Abel and Solvable Equations,* Arch. Hist. Exact Sci. 48 (1994), 81-103
10. L. Kronecker, *Über die algebraisch auflösbaren Gleichungen* (I), Monatsber. Berlin, 1853, 365-374 *Werke,* vol. 4, 3-11
11. L. Kronecker, *Über die algebraisch auflösbaren Gleichungen* (II), Monatsber. Berlin, 1856, 203-215 *Werke,* vol. 4, 25-37
12. P. M. Neumann, *The Mathematical Writings of Évariste Galois,* Peter M. Neuman, European Mathematical Society, Zurich, 2011
13. H. Weber, *Lehrbuch der Algebra,* Vieweg, Braunschweig, 1895 (Reprint, AMS/Chelsea)
14. A. Wiman, *Über die metacyklischen Gleichungen von Primzahlgrad,* Acta Math. 27 (1903) 163–175

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