Niels Henrik Abel and Solvable Equations

LARS GÅRDING & CHRISTIAN SKAU

Communicated by J. LÜTZEN

NIELS HENRIK ABEL proved in 1824 that the general equation of degree 5 cannot be solved by rational operations and root extractions starting with the coefficients. Two years later, in a letter to CRELLE, he gave explicit expressions of the roots of an equation of degree 5 which can be obtained in this way. He also announced that he had analogous results for any equation of prime degree. To substantiate this assertion, there is the posthumously published and unfinished manuscript (1828?) whose main part deals with solvable equations of prime degree. In addition, the introduction contains four statements about solvable equations in general of which indications of proofs are given at the end of the manuscript. After ABEL's death, when GALOIS' papers had been understood, the theory of solvable equations was tied up with the theory of solvable groups. Using the results by JORDAN (1870) in this area, WEBER was able to prove ABEL's statements (see WEBER's Algebra II (1895)) about the zeros and factorizations of the polynomials of solvable equations.

The purpose of this paper is to analyze ABEL's manuscript in the light of modernized versions and extensions of his proofs. The main tool is a normalization (Theorem 1) of the radical extensions of a ground field K to the splitting field $K(f)$ of an irreducible polynomial $f(x)$ with coefficients in K whose zeros can be obtained by successive root extractions. The theorem says that there is a tower of GALOIS fields

$$K \subset L_1 \subset \ldots \subset L_n = K(f)$$

for which each field is a primary extension of the previous one in that it is obtained by adjoining independent p^{th} roots of elements of the previous one, p a prime. The notion of a tower of GALOIS fields and primary extensions is implicit in a sheet of paper attached to ABEL's manuscript, but seems never to have been used effectively (see the Remark after Theorem 1).

For ABEL, the automorphisms of a splitting field of a solvable equation are generated by varying the arguments of n^{th} roots. We will of course use the notion of GALOIS group but always in connection with explicitly given fields. In this way we deviate from a pure tradition of group theory founded by C. JORDAN in his exposition (1870) of GALOIS theory and prevalent in the literature since then. In particular, Theorem 1 replaces one at the time knotty point of group theory, exposed for instance in WEBER (1895 II) s. 33–37, namely

that a solvable group has a commutative normal subgroup.[1] The paper ends with a short review of some papers from the beginning of this century by WIMAN and others on the structure of the zeros.

Our main result is perhaps that ABEL's paper gives a complete description of the roots a solvable equation of prime degree which was later ascribed to KRONECKER and WEBER. ABEL also has an explicit description of the GALOIS groups of such equations, although GALOIS's classical deduction of the GALOIS groups of metacyclic equations is simpler and slightly more general. The last pages of ABEL's manuscript show that he had a clear idea of the general case of solvable equations, in particular the primitive ones which remain irreducible in all GALOIS fields properly contained in its splitting field. It will be shown that SYLOW's reconstructions of ABEL's proofs of two of his general statements which concern solvable equations in general are perfectly valid and provide a simple alternative treatment by WEBER using group theory.

A version in Swedish of the part of this paper dealing with equations of prime degree was published in 1992 by one of us (GÅRDING 1992) who was led to the study of ABEL's paper (1828?) by MALMSTEN's elaboration of it (1847).

1. Preliminaries

The exposition will use modern terminology. When K is a field, let $K[x]$ denote the ring of polynomials with coefficients in K and when s belongs to a field over K, let $K(s)$ be the field of all rational functions of s with coefficients in K and similarly for $L = K(s_1, \ldots, s_n)$.

When $K \subset L$ are fields, let $\deg(L/K)$ denote the dimension of L as a linear space over K. A field L is said to be algebraic over a field $K \subset L$ if every $t \in L$ is algebraic over K in the sense that $n = \deg(K(t)/K)$ is finite. In this case t is a zero of a unique irreducible polynomial $x^n + \ldots \in K[x]$ also said to be the minimal polynomial of t over K. The other zeros of the polynomial are said to be conjugates of t over K. The notion of algebraic is transitive: if M is algebraic over L which is algebraic over K, then M is algebraic over K.

In what follows we shall restrict our treatment to fields of characteristic zero containing the rational numbers which are algebraic and of finite dimension over some fixed field, for instance the rationals, and contained in some other fixed algebraically closed field, for instance the complex numbers. It is well known that all the zeros of an irreducible polynomial $f(x)$ with coefficients in such a field are separate.

We shall use the notion of isomorphic mappings into an algebraically closed field. When a field L contains another one, K, and every isomorphism from

[1] In modern theory, this is proved by taking the sequence of successive commutator subgroups of a given group G. These subgroups are invariant and, if G is solvable, the sequence ends with unity. The preceding subgroup in the sequence has the desired property.

L which is the identity on K maps L into itself, *i.e.* is an automorphism of L, then L is said to be a GALOIS field over K. In this case, $\mathrm{Aut}(L/K)$ will denote the group of isomorphisms of L which are the identity on K. When $f(x) \in K[x]$ is irreducible with the zeros $x_1, \ldots, x_m$, its *splitting field* $K(x_1, \ldots, x_m)$ is a GALOIS field over K. For this field and its Galois group $\mathrm{Aut}(K(x_1, \ldots, x_m)/K)$ the simpler notations $K(f)$ and $\mathrm{Aut}(f/K)$ will be used. When K, K' are fields, $U: K \to K'$ is an isomorphism and t is algebraic over K and $f(x) \in K[x]$ the corresponding minimal polynomial, $K(t)$ is isomorphic to $K[x]/K[x]f(x)$. Hence if U maps $f(x)$ to $f'(x) \in K'[x]$ and t to t', the fields $K(t)$ and $K'(t')$ are isomorphic. Repeated applications of this remark gives the principle of

Extension. *When L is algebraic over K, every isomorphism from K extends to an isomorphism from L, the number of distinct extensions being* $\deg(L/K)$.

Let L be a GALOIS field over a field K and let M be a subset of L. From the extension principle follows the mainstay of GALOIS theory, more or less explicit in early work on the theory of equations, namely

Invariance. *Let H be the subgroup of* $\mathrm{Aut}(L/K)$ *which leaves all elements of M invariant. Then $t \in K(M)$ if and only if $Ut = t$ for all $U \in H$ where $K(M)$ denotes the smallest field containing K and M.*

In fact, if t is outside $K(M)$, t is algebraic over $K(M)$ and if $t_1, \ldots, t_n$ are the conjugates of t over $K(M)$ there is an element of

$$\mathrm{Aut}(K(M)(t_1, \ldots, t_n)/K(M))$$

which extends to $\mathrm{Aut}(L/K)$ and does not leave t invariant.

We can now prove a result, stated by ABEL ((1881) I, p. 547) and used by GALOIS (1831a, p. 36), namely the theorem of

One Generator. *If M is a field containing K, then $M = K(u)$ for a single element u.*

In fact, by hypothesis, $M = K(t_1, \ldots, t_n) = K(t_1)(t_2, \ldots, t_n)$, so that it suffices to consider the case $n = 2$, $M = K(s, t)$. Let $t_1, \ldots, t_k, \ldots,$ and $s_1, \ldots, s_k, \ldots,$ be all conjugates of s and t over K. Choose $c \in K$ such that c does not solve any equation $s_k + ct_j = s + ct$ with $t_j \neq t$. If U is any automorphism of a GALOIS field over K containing M such that $Uu = u$, $u = s + ct$, we have $s + ct = Us + cUt$ which is impossible unless $Ut = t$ and hence $Us = s$ so that $K(u) = K(s, t)$.

Finally, we shall prove a result which will be important later. In another form, it appears as proposition II of GALOIS (1831a) and in ABEL's unproven statement 3 of the introduction of his paper (1828?). In the form below it appears in WEBER I, 558–562.

Lemma A. *Suppose that* $f(x) \in K[x]$ *is irreducible and that*

$$f(x) = f_1(x) \ldots f_r(x)$$

splits into irreducible factors in a GALOIS *subfield* $M \subset K(f)$. *Then the factors have the same degree, the integer* r *divides* deg f *and there is an irreducible polynomial* $g(x) \in K[x]$ *of degree* r *such that* $f(x)$ *splits as above in* $K(g) \subset M$. *In particular, no polynomial* $f(x)$ *of prime degree splits in a proper* GALOIS *subfield of* $K(f)$.

Note. Since our fields have characteristic zero, the factors above are all different.

Proof. An element $U \in \mathrm{Aut}(M/K)$ either leaves (the coefficients of) a factor f_k invariant or transforms it to another factor. Hence the group $\mathrm{Aut}(M/K))$ permutes the factors above. Any product of factors which is invariant under this action must have coefficients in K. Since $f(x)$ is irreducible in $K[x]$, this means that the factors are permuted transitively. Hence all have the same degree so that r divides the degree of f. Let M_k be the field over K generated by the coefficients of the factor $f_k(x)$ and put $M_1 = K(u_1)$. The action of $\mathrm{Aut}(M/K)$ shows that $u = u_1$ has precisely r conjugates $u_1, \ldots, u_r$ such that $M_k = K(u_k)$. Hence if $g(x) \in K[x]$ is the minimal polynomial of u, deg $g = r$ and $K(g)$ is precisely the field generated by $M_1, \ldots, M_r$ over K and the lemma is proved.

2. Radical extensions and solvability of equations

When a field K contains a primitive n^{th} root of unity ω, the polynomial $x^n - a \in K[x]$ is irreducible and $t^n = a$, the field $K(t)$ is said to be a simple radical extension of K of degree n. The other zeros of $x^n - a$ are then $\omega t_1, \ldots, \omega^{n-1} t$ and $\mathrm{Aut}(K(t)/K)$ is cyclic and generated by the map $t \to \omega t$. The elements of $K(t)$ have the form $x_0 = g(t)$ where $g(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in K[x]$ has degree $< n$. The conjugates of x_0 are

$$x_k = a_0 + a_1 \omega^k t + \ldots + a_{n-1} (\omega^k t)^{n-1} \tag{1}$$

for $k = 0, \ldots, n-1$ and the terms a_k may be retrieved from LAGRANGE's resolvents

$$(\omega^j, x) = \sum_0^{n-1} \omega^{-jk} x_k \tag{2}$$

by the simple formula

$$n a_j t^j = (\omega^j, x) \tag{3}$$

When $n = mk$ is a product of integers, the radical extension $K \subset K(t)$ decomposes into two, $K \subset K(t^m) \subset K(t)$. It follows that a simple radical extension can

be decomposed into a sequence of *prime* extensions, *i.e.* simple radical extensions of prime degree.

A field L is said to be a radical extension of K if there is a sequence of simple radical extensions

$$K = K_1 \subset K_2 \subset \ldots \subset K_j = L \tag{4}$$

where we may assume that every field has prime degree over the preceding one. By definition we also require that K contains all the roots of unity which are required in the successive extension. (We could also assume from the beginning that K contains *all* roots of unity.)

A radical extension L of K is said to be a *primary* extension of L if $L = K(t_1, \ldots, t_m)$ where all $t_k^p \in K$ for some prime p but no t_k is a polynomial in the others with coefficients in K. It is clear that L is a GALOIS field over K. If $j = (j_1, \ldots, j_m)$ denotes multiindices mod p, the elements of L have the form

$$\sum c_j t^j, \quad t^j = \prod t_i^{j_i},$$

with unique coefficients $c_j \in K$. It follows that the group $\mathrm{Aut}(L/K)$ is generated by m commuting elements $T_1, \ldots, T_m$ such that $T_k t_i = t_i$ when $i \neq k$ and $T_k t_k = \omega t_k$ where ω is a primitive p^{th} root of unity. The elements of the group are all p^m powers T^j formed in the same way as t^j. Hence the number of elements of the group $\mathrm{Aut}(L/K)$ equals the primary degree p^m of L over K. The group itself is isomorphic to the additive group of Z^m mod p.

When K is a field and $f(x) \in K[x]$ is irreducible, the polynomial $f(x)$ and the equation $f(x) = 0$ are said to be solvable over K if the equation has a root in some radical extension of K. When this is the case, we shall see that the entire root field $K(f)$ is solvable in the sense that it is a radical extension of K. More precisely,

Theorem 1. *Suppose that $f(x) \in K[x]$ is irreducible and that the equation $f(x) = 0$ is solvable. Then there is a sequence of radical extensions*

$$K = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n = K(f), \tag{5}$$

where all fields are GALOIS *fields over K and every field is a primary extension of the preceding one.*

Remark. The sequence (5) will be called a (splitting) tower of $f(x)$ or $K(f)$ over K and the degrees $\deg(L_{j+1}/L_j)$ the indices of the tower. When $G_j = \mathrm{Aut}\,(K(f)/L_j)$, the corresponding (decreasing) tower of groups is

$$G_0 \supset G_1 \supset \ldots \supset E$$

where every group is normal in $G_0 = \mathrm{Aut}(f/K)$ and the successive quotients are commutative of primary order, specifically, a direct product of cyclic groups of some prime order. This kind of resolution, which exists for any solvable group, is called the chief or principal series in the modern literature (see SUZUKI (1982, 86),

vol II, p. 101). A tower of prime extensions leading from K to $K(f)$ is constructed for instance in VAN DER WAERDEN (1937) (p. 182), but the possibility of obtaining GALOIS fields under way is not mentioned.

It was pointed out by ABEL's editor SYLOW ((1881 II) p. 333) that ABEL's manuscript has a page (not printed there) where the successively adjoined radicals are ordered so that every line has radicals with the same prime order over rational functions of the preceding ones. Hence we may conclude that Theorem 1 apart from its terminology was in ABEL's mind. He did not use the concept of a group; instead he must have thought of the conjugates of a radical expression as obtained by varying the arguments of the radical involved. Theorem 1 is important for the understanding of ABEL's manuscript (1828?). The proof relies on three lemmas where it is understood that the field K contains a primitive p^{th} root of unity.

Lemma 1. *If $F(t)$ a prime extension of F of prime degree p then $F(bt^k) = F(t)$ when $0 \neq b \in F$ and $k \not\equiv 0 \bmod p$.*

Lemma 2. *With $F, F(t)$ as above, let $K \subset F$ and let $M \supset K$ be a GALOIS field over K. Then $F(t) \cap M = F \cap M$ or else there is a $t' \in F(t) \cap M$ such that $F(t') = F(t)$ and*

$$F \cap M \subset (F \cap M)(t') = F(t') \cap M$$

is a simple radical extension of $F \cap M$ of degree p.

Lemma 3. *Let L be a GALOIS field over K. Every prime extension $L(t)$ of L of degree p is contained in a GALOIS field over K in the form of a primary extension $M = L(t_1, \ldots, t_n)$ of degree p^k of L where $t^p = t_1^p, \ldots, t_k^p \in L$ are conjugates of t^p over K and no t_k is a polynomial in the others with coefficients in L.*

The proof of Lemma 1 is left to the reader. To prove Lemma 2, let (1), (2), (3) with $n = p$ refer to $F(t)$. If there is an element $u = g(t) \in F(t) \cap M$ which is not in F, we may use Lemma 1 to replace t by t' such that $F(t') = F(t)$ and

$$u = a_0 + t' + a_2 t'^2 + \ldots .$$

The conjugates of u over F are certainly in M. Hence $t' = (\omega, u)/p$ belongs to $F(t') \cap M$ and so do the other terms of the right side. We conclude that all the coefficients $a_0, a_2, \ldots$ belong to $F \cap M$. It follows that all the coefficients of an arbitrary $v = h(t') \in F(t') \cap M$ belong to $F \cap M$ and this proves Lemma 2.

To prove Lemma 3, let $b_1, \ldots, b_n$ be all conjugates of $a = t^p$ over K and let $s_i^p = b_i$ for $i = 1, \ldots, n$. Then every step in the sequence

$$L \subset L(s_1) \subset L(s_1, s_2) \subset \ldots \subset L(s_1, \ldots, s_n)$$

is an identity or a prime extension of order p and the last field is a GALOIS field over K. If $t_1, \ldots, t_k$ are those s_i which give increases in the sequence, we have

$$L(t_1, \ldots, t_k) = L(s_1, \ldots, s_n)$$

and all products

$$\prod_1^k t_i^{m_i}$$

with $0 \leqq m_i < p$ form a basis of $M = L(t_1, \ldots, t_k)$ over L which then is a primary extension of L of dimension p^k over L.

Proof of Theorem 1. Apply Lemma 2 with $M = K(f)$ in steps from right to left in a sequence (4) with L containing a root of $f(x) = 0$. It follows that there is a similar sequence with all fields contained in $K(f)$. An application of Lemma 3 from left to right in this sequence finishes the proof.

Corollary 1. *When $f(x) \in K[x]$ is irreducible and solvable, any* GALOIS *field between K and $K(f)$ is itself solvable and part of a tower of $f(x)$. When $f(x)$ splits into r irreducible factors in a* GALOIS *field of a tower, it splits in the same way in a field $K(g) \subset K(f)$ where $g(x) \in K[x]$ is solvable and of degree r. When the polynomial $f(x)$ is primitive in the sense that it does not split in any* GALOIS *field properly contained in $K(f)$, its degree is primary and equals the last index of a splitting tower.*

Remark. The term primitive was introduced in GALOIS (1831b) and is implicit in ABEL's manuscript. According to WEBER a transitive permutation group is primitive when it does not have a proper intransitive normal subgroup.

Proof. Suppose that $M \supset K$ is a GALOIS field contained in $K(f)$ and that $f(x)$ has the tower (5). By Lemma 2, the intersections

$$K = K \cap M \subset L_1 \cap M \subset \ldots \subset K(f) \cap M = M$$

can be shortened to a tower of M over K. By adjoining to M all the p^{th} roots in the order they appear in (5), we get a tower from M to $K(f)$ and hence a tower of $K(f)$ over K of which M is a part. The second statement follows from Lemma A. When $f(x)$ is primitive, it remains irreducible in the field $L = L_{n-1}$ of a tower (5) and splits into linear factors in $K(f)$. These factors are permuted transitively by $G = \mathrm{Aut}(K(f)/L)$ which has order p^m for some prime p. Hence the number of factors divides p^m and so is primary. If one element of G leaves one factor invariant it leaves all invariant since G is commutative and so must be the identity. Hence the number of factors is precisely p^m. This finishes the proof.

A statement by Abel

The nature of the factorization of polynomials with solvable equations was known to ABEL and expressed in the introduction of (1828?) as a statement with the number 3.

3 *If an equation of degree μ which is divisible by different primes is algebraically solvable, it is always possible to decompose μ into two factors μ_1 and μ_2 so that the original equation is decomposed into μ_1 equations, each one of degree μ_2 whose coefficients depend on equations of degree μ_1.*

We may assume that the equations in question is $f(x) = 0$ where $f(x) \in K[x]$ is solvable. If the degree of the polynomial $f(x)$ is not primary, Corollary 1 shows that it cannot be primitive and hence splits in some term of one of its towers (5). If the number of factors is $r = \mu_1$, Lemma A and the first part of Corollary 1 exhibit the situation described by ABEL. (His equations of degree $r = \mu_1$ may refer to the fields $K(u_k)$ which generate the coefficients of the factors $f_k(x)$ of Lemma A.) ABEL's statement is an example of his deep insight into the workings of the machinery of algebraic fields.

3. Solvable equations of prime degree

ABEL's manuscript (1828?) starts with fully edited generalities about radical extensions but the main part, where the subject is solvable equations of prime degree, is more of a sketch. The purpose of this section is to supply proofs in the spirit of ABEL of the results about solvable equations of prime degree which he states and, more or less explicity proves. All our fields are supposed to contain the rational numbers.

Theorem 2. *Let p* be a prime, *K be a field containing the p^{th} roots of unity and let $f(x) \in K[x]$ be irreducible of prime degree p. If the equation $f(x) = 0$ is solvable, there is a* GALOIS *field L over K with a prime extension $L(t)$ of degree p such that*

(i) $K(f) = K(t)$,

(ii) $L = K(s)$, $s = t^p$,

(iii) *the roots* $x_0, \ldots, x_{p-1}$ of $f(x) = 0$ *have the form*

$$x_k = \sum_0^{p-1} a_j \omega^{kj} t^j, \quad a_j t^j = p^{-1}(\omega^j, x) \tag{6}$$

where $a_j = a_j(s)$ with $a_j(x) \in K[x]$, $a_1 = 1$ and ω is a primitive p^{th} root of unity.

Remark. Note that $a_0 = (x_0 + \ldots + x_{p-1})/p$ belongs to K.

Proof. In a tower (5), $f(x)$ can only split in the last step and then into linear factors. Hence, by the last part of Corollary 1, the last step of (5) has index p and we have radical extensions

$$K \subset L \subset L(t) = K(f),$$

where t is a zero of an irreducible polynomial $x^p - s \in L[x]$ and $L = L_{n-1}$ is a GALOIS field over K. From this (6) follows immediately with $a_j \in L$ since Lemma 1 shows that we may choose t such that $a_1 = 1$.

Suppose now that $U \in \mathrm{Aut}(f/K)$ and that $Ut = t$. Note that $UL = L$. By (6) the zero x_k is uniquely determined by being a linear combination with coefficients in L of the powers of t with ω^k the coefficient of t. Hence, if $U \in \mathrm{Aut}(f/K)$ and $Ut = t$ then $Ux_k = a_0 + \omega^k t + \ldots$ can only be x_k. This proves that U is the identity so that (i) follows and since L consists of all elements of $K(t)$ which are invariant under $t \to \omega t$, (ii) follows. Now (ii) in conjunction with the above implies (iii).

We can now prove two corollaries which together contain all that ABEL desired to prove.

Corollary 2. *Every* $U \in \mathrm{Aut}(f/K)$ *has the form*

$$Ut = a(s)t^k \tag{7}$$

where $a(x) \in K[x]$ *and* $k \equiv |0 \bmod p$. *The effect on non-vanishing* LAGRANGE'S *resolvents*

$$(\omega^j, \mathrm{x}) = \sum_0^{p-1} \omega^{-ji} x_i \tag{8}$$

is given by

$$U(\omega^j, x) = \omega^{jki}(\omega^{jk}, x) \tag{9}$$

where $Ux_0 = x_l$.

Proof. Define $T \in \mathrm{Aut}(K(f)/L) \subset \mathrm{Aut}(f/K)$ by $Tt = \omega t$ which implies that $Ts = s$. Note that, by (6), $Tx_i = x_{i+1}$, the indices taken mod p. To prove (7) note that $(TUt) = TUt^p = Us$ since $UK(s) = K(s)$. Hence Ut and TUt both solve the equation $x^p - Us = 0$ so that $TUt = \omega^k Ut$ for some k. Since Ut is a polynomial in t with coefficients in $L = K(s)$, this is only possible if (7) holds. By (3), $K(s)$ playing the role of K,

$$pa_j t^j = (\omega^j, x). \tag{3'}$$

Hence all non-vanishing resolvents are linearly independent over $K(s)$ and (7) and (3') show that U maps every non-vanishing (ω^j, x) into $c_j(\omega^{jk}, x) \neq 0$, $c_j \in L$. In particular, if $Ux_0 = x_0$ (note that px_0 is just the sum of the resolvents), all

c_j are one and U permutes the nonvanishing resolvents. If $Ux_0 = x_l$, $V = T^{-l}U$ maps x_0 into itself and hence $U = T^l V$ acts as described in (9).

The Galois groups $\mathrm{Aut}(f/K)$ *and* $\mathrm{Aut}(K(s)/K)$

The formula (9) gives a complete description of $\mathrm{Aut}(f/K)$ by its action on the resolvents. We can also show that the group $\mathrm{Aut}(K(s)/K)$ is cyclic of an order r which divides $p-1$. In fact, since $s = t^p$ and $K(s)$ is precisely the part of $K(t)$ which is invariant under the translation operator T, the group $\mathrm{Aut}(K(s)/K)$ equals $\mathrm{Aut}(f/K)$ mod T. Hence it is isomorphic to the subgroup G of $\mathrm{Aut}(f/K)$ which leaves x_0 invariant. According to (9) this group is isomorphic to a subgroup of the multiplicative group Z_p^* and hence has the property stated.

Behind the formula (9) there is also an explicit description of $\mathrm{Aut}(f/K)$ as isomorphic to a subgroup of the affine group Γ of affine maps

$$j \to ij + l \mod p.$$

In fact, if $kk' \equiv 1 \mod p$, (9) reads

$$Ux_j = x_{jk'+l} \tag{9'}$$

where the indices are to be taken mod p. To see this is a matter of pure computation but we may also go directly from (7) which says that $UT = T^{k'}U$ so that by iteration $UT^j = T^{jk'}U$. Applying this identity to x_0 gives (9').

In this way (9') appears as a special case of a famous theorem by GALOIS (1831a) which characterizes $\mathrm{Aut}(f/K)$ in the same way when the equation $f(x) = 0$ of prime degree p is metacyclic in the sense that $K(f)$ is the first field to split $f(x)$ in a sequence

$$K = L_0 \subset L_1 \subset \ldots \subset L_n = K(f),$$

where every $\mathrm{Aut}(L_{k+1}/L_k)$ is cyclic. GALOIS's simple proof proceeds by induction. $\mathrm{Aut}(L_n/L_{n-1})$ is cyclic of order p and every element in Γ of order p must belong to the maximal cyclic subgroup generated by the translation T: $j \to j+1$. If $\mathrm{Aut}(L_n/L_j)$ is isomorphic to a subgroup of Γ and $U \in \mathrm{Aut}(L_n/L_{j-1})$ then UTU^{-1} has order p and is the identity on L_j so it must be a power of T. We can then continue as above to prove that also $\mathrm{Aut}\,(L_n/L_{j-1})$ is isomorphic to a subgroup of Γ.

Fixing the zeros

Both GALOIS and ABEL stressed the fact that all zeros of $f(x) = 0$ are rational functions of two of them, or, equivalently, that no element of $\mathrm{Aut}(f/K)$ can fix two zeros without reducing to the identity. The proof is obvious from any of the two presentations (9) or (9'). GALOIS even saw this property as characteristic of subgroups of the affine group Γ mod p.

The form of the zeros of $f(x) = 0$

Let U be a generator of the subgroup G of $\mathrm{Aut}(f/K)$ which leaves x_0 invariant. Then by (7),

$$Ut = c(s)t^g \tag{10}$$

where $c(s) \in K(s)$ and $g^r \equiv 1 \bmod p$ but not for any lower powers of g.

Let $B_i = \bigcup_0^{r-1}(\omega^{ig^h}, x)$ be the G-orbit of $(\omega^i, x) \neq 0$ where $i \not\equiv 0 \bmod p$. The orbit must have r elements since all ig^k are different mod p. Let I be a subset of $(1, \ldots, p-1)$ such that

$$\bigcup_{i \in I} B_i \tag{11}$$

partitions the nonvanishing resolvents into orbits under U. Our next Corollary is ABEL's main result and can be found in (1828?) on top of p. 240.

Corollary 2B. *There is an element* $U \in \mathrm{Aut}(f/K)$ *whose order* r *divides* $p-1$ *and such that*

$$Ut = a(s)t^g, \quad Us = a(s)^p s^g \tag{12}$$

and the zeros of $f(x) = 0$ *are given by*

$$px_0 = a_0 + \sum_{i \in I} \sum_{k=0}^{r-1} c_{ik}(\sqrt[p]{s})^{ig^k} \tag{13}$$

with $c_{ik} \in K(s)$ *when* $\sqrt[p]{s}$ *assumes its* p *values.*

Proof. The formula (12) is a restatement of (10) and (13) follows from (6), (3′) and (11). When $\sqrt[p]{s}$ is multiplied by ω^j, the left side of (13) changes to px_j.

Remark. With ABEL we can get equivalent forms of the orbits of (13) where $\sqrt[p]{s}$ is replaced by another expression where r different resolvents multiplied by elements from $K(s)$ can change their arguments without producing more than p zeros. It suffices to assume that $a_1 = 1$, hence $pt = (\omega, x)$, and illustrate this for the orbit

$$t, Ut, \ldots, U^{r-1}t. \tag{14}$$

Let us first remark that we may assume that

$$1 - g^r = p - qp^2 . \tag{15}$$

In fact, if $g^r \equiv 1 + jp \bmod p^2$, we may substitute $g + kp$ for g and then (15) is brought about by a suitable choice of k.

If we write the terms of (14) explicitly we get

$$t, a(s)t^g, a(Us)\,a(s)^g t^{g^2}, \ldots, a(U^{r-2}s)\,a(U^{r-3}s)^g \ldots a(s)^{g^{r-2}} t^{g^{r-1}}.$$

In the next step $t = B(s)t^{g^r}$ where

$$B(s) = a(U^{r-1}s)\,a(U^{r-2}s)^g \ldots a(s)^{g^{r-1}}. \tag{16}$$

Hence by (15)

$$t = A(s)\sqrt[p]{B(s)},\quad A(s) = s^q$$

so that

$$U^k t = A(U^k s)\sqrt[p]{B(U^k s)} \tag{17}$$

and hence

$$t + Ut + \ldots + U^{r-1}t = \sum_0^{r-1} A(U^k s)\sqrt[p]{B(U^k s)}.$$

This is precisely the form found by ABEL in (1826b) for the roots of a solvable equations of degree 5. Note that U operates on the product B by cyclically translating the exponents.

4. Analysis of Abel's manuscript

In this section, which is a critical analysis of ABEL's manuscript, we shall use the notations of the preceding section. The symbol s has the same meaning in both cases. Our p, t are ABEL's $\mu, s^{1/\mu}$.

On p. 233 of (1881 II) ABEL starts his analysis of solvable equations of prime degree p and finds that the zeros have the form

$$x_k = a_0 + a_1\omega^k t + \ldots \omega^{k(p-1)}t^{p-1} \tag{A.1}$$

for $k = 0, \ldots, p-1$ and $t = \sqrt[p]{s}$ with s in the same field as the coefficients $a_0, a_1, \ldots$. He then subjects the zeros and the right sides to an operation in $\mathrm{Aut}(f/K)$, putting $Us = s'$, $Ua_k = a_k'$. Eliminating the zeros x_k he deduces from this that s' is a polynomial in $s^{1/p}$ whose coefficients are rational functions of the a_k and a_k'. He desires to conclude from this that no fractional power of s occurs and argues that, in the opposite case, $s^{1/p}$ and hence x_0 would be a rational function of s, a_k, s', a_k'. If this holds, s', a_k' cannot be rational functions of s, a_k for this would imply the same for $s^{1/p}$. Then, considering the irreducible equation satisfied by x_0 with s', a_k' not rational functions of s, a_k, ABEL says that it cannot have prime degree. (May be he thinks of the situation described in Lemma A. Anyway, without amplification, the argument does not hold water).

In his extended analysis of ABEL's manuscript (1881 II, 332-335), SYLOW objects to this wholesale argument and points out the remedy described in the remark after Theorem 1.

Having accepted, essentially, that the field L of the coefficients a_k is a GALOIS field, ABEL proceeds on p. 235 to prove our basic formula (7) for the action of $U \in \mathrm{Aut}(f/K)$, *i.e.*

$$Ut = at^k \tag{A.2}$$

for some $a \in L$ and $k \not\equiv 0 \mod p$. Identifying the coefficient of t^k in $Ux_0 = x_1$ (which is assumed in the process) he then states that

$$U(a_1 t) = \omega^k a_k t^k \tag{A.3}$$

from which he draws the conclusion that $a_1^p s$ has at most $p-1$ values and hence satisfies an equation of at most degree $p-1$. As we have seen, this is true for all elements of $L = K(s)$.

At this point, ABEL has all but proved (9) of Corollary 2A, repeated here,

$$U(\omega^j, x) = \omega^{jkl}(\omega^{kj}, x). \tag{9}$$

In fact, the reasoning that gave (A.3) also gives

$$U(a_j t^j) = \omega^{jk} a_{jk} t^{jk}$$

with jk taken mod p and, since $a_j t^j = (\omega^j, x)/p$, this is precisely (9) when $Ux_0 = x_1$. If $Ux_0 = x_l$, we get (9) by applying an appropriate power of the translation operator.

All this is very well, but ABEL has not really proved (A.2) since he has no good proof that $L = K(s)$. But in his next step ABEL tries to show that the coefficients a_k of (A.1) belong to $K(s)$. Assuming $a_1 = 1$, ABEL can express the resolvents t and $a_k t^k$ as polynomials in the zeros $x_0, \ldots, x_{p-1}$ with coefficients in the ground field. Hence the same holds for any $q = a_k s^j$. Taking a sum over v conjugates and putting $j = 0, \ldots, v-1$ he gets a system of linear equations for the conjugates $q_1, \ldots, q_v$ of q with a VAN DER MONDE determinant given by the corresponding conjugates $s_1, \ldots, s_v$ of s. Solving the system shows that q_1 is a polynomial in $s_1, \ldots, s_v$ which is symmetric in $s_2, \ldots, s_n$ and hence q is a polynomial in s. (ABEL's text is now getting less and less precise. All his troubles stem from the fact that he has not discovered the easy proof that $K(f) = K(t)$ but since he has now shown that all the coefficients a_k of (A.1) are in $K(s)$, he has finally arrived at this basic conclusion.)

In the lower part of p. 237, ABEL assumes that the resolvents are in $K(t)$ and explores the consequences of the key equation (A.2) raised to the p^{th} power. Iterations m times lead to expressions

$$f_m(s) s^{k^m}$$

which eventually will lead back to s. Since $k^{p-1} \equiv 1 \mod p$, ABEL thinks that this will happen for m a factor of $p-1$. This is ultimately correct but cannot be obtained in this way since, in contrast to the powers of t, the powers of s are not linearly independent over polynomials in s. However, the same computations in terms of powers of t show that the conclusion is correct.

What is missing at this point is some argument that every element U of $\mathrm{Aut}(f/K)$ permutes the p^{th} powers of the resolvents cyclically according to (9). Note that only the non-vanishing ones are involved.

On p. 238 and 239 ABEL experiments with generators of $\mathrm{Aut}(K(s)/K)$ and at the bottom of p. 239, he has concluded (but not proved!) that the operations

of $\mathrm{Aut}(f/K)$ on the p^{th} powers of the resolvents are generated by a single element.

$$Us = a(s)^p s^g$$

for which he writes down the iterates. Without any explanation he then writes down the big formula on top of p. 240 which is the same as (13) of Corollary 2B. Our g is ABEL's m^α, m being of order $p-1$ in the multiplicative group mod p and our r is ABEL's ν. On the bottom part of the page he writes down what amounts to the formula (16). The page 240 has in it the complete theory of solvable equations of prime degree p, both the possible GALOIS groups and the form of the zeros.

To sum up this analysis: In this manuscript ABEL has guessed and partly proved the entire theory later ascribed to KRONECKER and WEBER. Moreover, the theorem by GALOIS applied to solvable equations of prime degree is included implicitly. The flaw of ABEL's arguments is his complicated proof that, in our notations, $K(f) = K(t)$ ((i) of Theorem 2). Like us he could have obtained an easy proof by the invariance principle, which was known to him.

5. Malmsten, Kronecker, Weber

MALMSTEN's article (1847) is an elaboration of ABEL (1828?). MALMSTEN follows ABEL's text rather faithfully except for ABEL's system of formulas on the top part of p. 234. These are written out in full by MALMSTEN (p. 70) who agrees that the coefficients in

$$x_0 = a_0 + a_1 t + \ldots + a_{p-1} t^{p-1}$$

are polynomials in $s = t^p$. With t a conjugate of t, he finds that

$$a(s')t'^k = \sum c_{kj} a_j(s) t^j$$

for some numerical coefficients c_{kj}. He now claims that the p^{th} power of the left side does not contain $s^{1/p}$ and hence, in our language, is invariant under $t \to \omega t$. (At this point MALMSTEN implicitly assumes that $K(s)$ is a GALOIS field.) From this he concludes quite rightly that the map $t \to \omega t$ on the right must multiply the left by a power of ω. Hence the right side has just one term, say $c_{kj} a_j(s) t^j$. Using the argument above, he shows that c_{kj} is a power of ω. This does not affect the p^{th} power and MALMSTEN can conclude that $\mathrm{Aut}(f/K)$ simply permutes the p^{th} powers of the non-vanishing resolvents $(\omega, x), \ldots, (\omega^{p-1}, x)$.

This is MALMSTEN's final result and he uses it to prove that a general equation of prime degree > 3 cannot be solved by root extractions and rational operations. The argument here is very simple. For a general equation, we may assume that the zeros $x_0, \ldots, x_{p-1}$ are independent symbols. This makes the resolvents linear forms in these symbols, so none of them are vanishing. If the equation were solvable, the product of the p^{th} powers of the resolvents would be invariant but it is easy to see by *e.g.* exchanging x_0 and x_1 that this gives a contradiction unless $p = 3$.

In the introduction to his first article (1853) on solvable equations KRONECKER quotes ABEL and MALMSTEN and announces (1853, p. 6) as his own the discovery that $\mathrm{Aut}(f/K)$ induces a cyclic permutation of the p^{th} powers of the resolvents. As said above, this is stated implicitly by ABEL in (1828?) but KRONECKER quotes from ABEL just two formulas from which this fact is not apparent. He also writes down (p. 6) what amounts to the formula (13) of Corollary 2B for the p^{th} powers of the resolvents, but he does not seem to have noticed that the same expression appears in ABEL (1828?) after the basic formula on top of p. 240. The explanation may be that he has preferred the clear and well edited manuscript by MALMSTEN to ABEL's sometimes confusing text. In his next article (1856) KRONECKER uses the fact that, if $f(x) = 0$ is solvable, only the identity in $\mathrm{Aut}(f/K)$ can leave two zeros invariant to prove that if $f(x)$ has real coefficients, it can only have 1 or p real zeros. Further on, he is on his way to the study of solvable equations with an abelian GALOIS group, in particular those with integral coefficients.

When SYLOW (1881 II p. 336) says that KRONECKER completed ABEL's investigations, he knows better. He was more outspoken in his article (1861) where he tried to prove ABEL's introductory general statements, analyzed at the end of this paper. There he says that KRONECKER's formulas are due to ABEL but also that he himself had only recently been able to understand ABEL's manuscript.

The entire theory of solvable equations of prime degree was taken up in WEBER's textbook (1895). The novelty here is the use of GALOIS's theorem to deduce immediately the action of $\mathrm{Aut}(f/K)$ on the resolvents. With this step, the problem to prove that the field L of Theorem 2 is a GALOIS field vanished temporarily from the mathematical literature, but as we shall see below, it reappears for solvable equations of primary degree.

6. Solvable primitive equations

ABEL's paper (1828?) does not deal only with solvable equations of prime degree. In the introduction (p. 222 of (1881 II)), ABEL stated the problem of solvable equations as follows.

Which is the most general radical expressions which can be a zero of an algebraic equation of a given degree?

This statement is followed by four other statements about the structure of the zeros of irreducible and solvable equations. The first one is concerned with equations of prime degree, the others of which there are no proofs in the manuscript, only some scribbles (1881 II, p. 241–43), deal essentially with equations of primary degree.

An extension of Theorem 2

Before reproducing and commenting on ABEL's statements, we shall use Theorem 1 to state and prove an extension of Theorem 2 and Corollary 2A for

primitive solvable equations $f(x) = 0$, where $f(x) \in K[x]$ is irreducible. If (5) is the associated tower, Theorem 1 and Corollary 1 show that $f(x)$ is irreducible in $L = L_{n-1}$ and factors into linear factors in $L_n = K(f)$. Further,

$$K(f) = L(t_1, \ldots, t_m)$$

is a primary extension of degree p^m of L, p a prime. The elements of $K(f)$ have the form,

$$c = \sum c_j t^j, \quad t^j = \prod t_i^{j_i}, \quad c_j \in L$$

where the components of $j = (j_1, \ldots, j_m)$ are integers mod p. The elements of the group $\mathrm{Aut}(K(f)/L)$ are similarly defined products T^k of pairwise commuting generators $T_1, \ldots, T_m$ with the action $T^k t^j = \omega^{(k,j)} t^j$, where $(k,j) = \sum_1^m k_i j_i$. Hence the p^m zeros have the form

$$x_k = T^k x_0 = \sum a_j T^k t^j = \sum \omega^{(k,j)} a_j t^j \tag{18}$$

where

$$a_j t^j = p^{-m}(\omega^j, x), \quad (\omega^j, x) = \sum \omega^{-(k,j)} x_k, \tag{19}$$

the last equation being the definition of the resolvent (ω^j, x). Observe that $T^l x_k = x_{k+l}$, the indices taken mod p, and that $T^l(\omega^j, x) = \omega^{(l,j)}(\omega^j, x)$.

Theorem 3. *If $f(x) \in K[x]$ is primitive and solvable, there is a radical sequence (5) such that $f(x)$ is irreducible in $L = L_{n-1}$ with $K(f) = L(t_1, \ldots, t_m)$ a primary radical extension of L of dimension p^m, p a prime, which is also the degree of $f(x)$. Further,*

$$K(f) = K(t_1, \ldots, t_m), \quad L = K(s_1, \ldots, s_n), \quad s_k = t_k^p. \tag{20}$$

The zeros of $f(x)$ have the form

$$x_k = \sum a_j \omega^{(k,j)} t^j, \quad a_j t^j = p^{-m}(\omega^j, x) \tag{21}$$

with $a_j \in L = K(s_1, \ldots, s_m)$.

Remark. By the construction of a tower, $s_1, \ldots, s_m$ are conjugates of s_1 over K. The form (21) of the zeros is by no way unique. In fact, we may exchange them for a set of conjugates. It will be seen later that there is a choice which makes the zeros symmetric in $t_1, \ldots, t_m$ modulo actions of $\mathrm{Aut}(K(f)/L)$ (to Abel, Statement 4 below).

Proof. If $U \in \mathrm{Aut}(f/K)$ leaves all t_i invariant and $Ux_0 = x_k$, then

$$\sum U a_j t^j = \sum a_j \omega^{(k,j)} t^j$$

so that $U a_j = \omega^{(k,j)} a_j$ for all j and then, since $UL = L$,

$$U x_i = \sum a_j \omega^{(k+i,j)} t^j = T^k x_i$$

so that $U = T^k$ on $K(f)$. But this is possible only when $k = 0$ and so U is the identity. Hence the first equality of (20) follows and the second one follows since L is the part of $K(t_1, \ldots, t_m)$ invariant under all T^k (*cf.* the proof of Theorem 2). The formula (21) now follows from the two previous ones.

Corollary 3. *The action of an element* $U \in \mathrm{Aut}(f/K)$ *is given by*

$$U(\omega^k, x) = \omega^{(Ak,j)}(\omega^{Ak}, x) \tag{22}$$

where A is an $m \times m$ *invertible matrix of integers* $\bmod p$ *and* $Ux_0 = x_j$.

Remark. The formula above means that $\mathrm{Aut}(f/K)$ is a subgroup of the affine group of Z_p^m which contains all the translations. The action of U on the zeros x_k is easily seen to be $Ux_k = x_{Bk+j}$ where B is the inverse transpose of A. In this form the result is quite explicit in GALOIS (1831b). A new choice of generators t_i as in the remark after Theorem 3 subjects the matrices A to a similarity transformation $\bmod p$.

Remark. It follows that an affine subspace of Z^m invariant under an element $U \in \mathrm{Aut}(f/K)$, considered as an affine map of Z_p^m, has one of the dimensions $1, \ldots, m$. In particular, if the coefficients of $f(x)$ are real, U may be complex conjugation and hence the possible number of real zeros (corresponding to the eigenvalue 1) are $1, p, \ldots, p^m$ when p is odd and $0, 2, \ldots, 2^m$ when $p = 2$. For $m = 1$, this was first observed by KRONECKER (1856) and in the general case by MAILLET (1904), DICKSON (1905) and BUCHT (1909).

To prove the corollary, ABEL's key argument in the proof of Corollary 2A will be used again. We state it as a lemma.

Lemma B. *If* $c \in K(f)$ *and* $c^p \in L$ *then* c *has the form* $c_j t^j$ *for some* $c_j \in L$.

Proof. We may assume that $c \neq 0$. Since $(T^k c)^p = T^k c^p = c^p$ we have $(T^k c/c)^p = 1$ and hence $T^k c = w^{B(T^k)} c$ for some $B(T^k)$. Since $T^k \to B(T^k)$ is obviously multiplicative, $B(T^k) = (k, j)$ where $j_i = B(T_i)$. Hence c must have the form $c_j t^j$ since $T^k t^j = w^{(k,j)} t^j$ and so $T^k(c/t^j) = c/t^j$ for all k.

Proof of Corollary 3. By Lemma B,

$$Ut_i = c_i t^{\alpha_i}, \quad \alpha_i = (a_{1i}, \ldots, a_{mi}) \mod p$$

for some $c_i \in L$ and hence $Ut^k = ct^{Ak}$ for some $c \in L$ where $A = (a_{li})$. Hence, by (19), U permutes the non-vanishing resolvents according to (22) modulo multiplication by elements of L. Now if $Ux_0 = x_j$, then $V = T^{-j}U$ has the property that

$$Vx_0 = x_0 = \sum (Va_j) t^{Aj}, \quad x_0 = \sum a_j t^j$$

where $j \to Aj$ is a bijection and the coefficients of the various powers t^j must be those of x_0. Hence $Va_j = a_{Aj}$ and (22) follows for $U = V$ and $j = 0$. But then it follows in general.

Abel's statements in light of Theorem 3

Now let us look at ABEL's statements, which he numbered from 1 to 4. The first one concerned with solvable equations of prime degree has been completely analyzed in Section 3 and his third statement has been analyzed in connection with Theorem 1. Translated into English and with numbering of the formulas added, the others are:

2. *If an irreducible equation whose degree μ^α is a power of prime number μ is algebraically solvable, two situations may occur; either the equation is decomposable into $\mu^{\alpha-\beta}$ equations, each of degree μ^β whose coefficients depend on an equation of degree $\mu^{\alpha-\beta}$, or it is possible to express any of its zeros as*

$$y = A + \sqrt[\mu]{R_1} + \sqrt[\mu]{R_2} + \ldots + \sqrt[\mu]{R_\nu} \tag{A.3}$$

where A is a rational quantity and $R_1, \ldots, R_\nu$ are zeros of an equation of degree ν, this number being at most $\mu^\alpha - 1$.

4. *If an irreducible equation f degree μ^α, μ a prime, is algebraically solvable, it is always possible to express anyone of its zeros by the formula*

$$y = f(\sqrt[\mu]{R_1}, \sqrt[\mu]{R_2}, \ldots, \sqrt[\mu]{R_\alpha}), \tag{A.4}$$

where f denotes a rational and symmetric function of the roots within parenthesis and $R_1, \ldots, R_\alpha$ are zeros of an equation whose degree is at most $\mu^\alpha - 1$.

Remark. ABEL assumes implicitly that the equation of Point 4 is primitive.

The first informed commentary to all these points is due to SYLOW (1861) who also compared them to GALOIS's work. Relying on the form of its roots, he gives a proof that a solvable primitive equation has primary degree and he states without proof that the coefficients of (21) are rational functions of $s_1, \ldots, s_m$. At this time, however, he passes over a difficulty he shall discover in his commentary on ABEL's collected works, namely, the subfields of the splitting field he considers must be GALOIS fields for the arguments to make sense.

We shall comment ABEL's statements in light of Theorem 3. The first part of Point 2 is Lemma A applied to an imprimitive irreducible polynomial of primary degree. The second part follows from Theorem 3. The R_k of (A.3) are the p^{th} powers of the non-vanishing resolvents except (w^0, x). This means of course that ABEL must have had an idea of the corresponding GALOIS group. The entities $R_1, \ldots, R_\alpha$ of Point 4 must be the $s_1, \ldots, s_m$ of Theorem 3 or, rather, since

they are roots of the same equation, a collection of m p^{th} powers of non-vanishing resolvents which generate $K(f)$ over L. Using our notations, it suffices to take a collection of m non-vanishing terms $a_k t^k$ of (21) such that the exponents k serve as a basis of Z_p^m. ABEL says that the right side of (A.4) is symmetric in his variables. We shall see below that $s_1, \ldots, s_m$ can be chosen to achieve this.

Sylow's reconstruction of Abel's proofs of 2 and 4

Point 4 (where it is implicitly assumed that the equation is primitive) is remarkable because ABEL's proof of the corresponding statement when $m = 1$, namely that the zeros are rational functions of t ((i) of Theorem 2), is very laborious and seems difficult to extend to the general case. But since he said that his statements are results obtained, they must be more than mere guesses from the case $m = 1$. That this is so is clear from SYLOW's reconstruction of ABEL's proof.

At the end of ABEL's manuscript there are some formulas with a sparse text. His commentator SYLOW has interpreted the text as proofs of the statements 2 and 4 above (1881 II, p. 336–37). They can be paraphrased as follows where $f(x) = 0$ is a solvable equation with coefficients in a field containing the necessary roots of unity, say the field K. There is a GALOIS field L over K such that $f(x)$ is irreducible in $L[x]$ but splits into irreducible factors,

$$f(x) = g(t, x)g(\omega t, x) \ldots g(\omega^{p-1}t, x)$$

in $L(t)[x]$ where $L(t)$ is a prime extension L of prime degree p. When $\mathrm{Aut}(f/K)$ operates on this splitting we get m copies of it,

$$f(x) = g_i(t_i, x)g_i(\omega t_i, x) \ldots g_i(\omega^{p-1}t_i, x), \quad i = 1, \ldots, m,$$

where $t_1, \ldots, t_m$ are conjugates over K of $t = t_1$. ABEL considers the greatest common divisor

$$g_k(x), \; k = (k_1, \ldots, k_m),$$

of

$$g_1(\omega^{k_1}t_1, x), g_2(\omega^{k_2}t_2, x), \ldots, g_m(\omega^{k_m}t_m, x). \tag{23}$$

There are p^m different such divisors conjugate under $\mathrm{Aut}(L(t_1, \ldots, t_m)/L)$ and hence of the same degree r. Now $g_k(x)$ is irreducible in $M[x]$, where $M = L(t_1, \ldots, t_m) \subset K(f)$ is a GALOIS field over K, and $f(x) = c\prod g_k(x), c \in K$. Lemma A then proves the first statement of 2. Under the second assumption of 2., $f(x)$ is primitive so that $r = 1$ and each factor $g_k(x)$ must be linear. In our notation, $g_k(x)$ equals $x - x_k$ where x_k is given by Theorem 3 and so the second statement of 2. follows by Corollary 3. Note that

$$g_i(w^{k_i}t_i, x) = \prod_{j_i = k_i} (x - x_j).$$

To all this there is the fact that each g_k is uniquely determined by the choice of $t_1, \ldots, t_m$ (and k). Hence, by the invariance principle, each x_k is a polynomial in $t_1, \ldots, t_m$ with coefficients in K. This proves the statement 4 except the symmetry. Precisely this invariance argument in a simpler setting was used above in the proofs of Theorem 2 and 3. It is a safe guess that ABEL would have used it also for Theorem 2 if he had been able to finish his paper. ABEL's tacit assumption that L is a GALOIS field is justified by our Theorem 1 which in turn was inspired by ABEL's way of ordering the successive adjungation of roots of prime order to form a tower of GALOIS fields.

About the symmetry. We reproduce SYLOW's arguments. With $t_1, \ldots, t_m$ as above, put $t = t_1$. Since L is a GALOIS field over K, the group $\mathrm{Aut}(L(t)/K)$ permutes the factors of the following factorization of $f(x)$ in $L(t)$,

$$f(x) = \prod_0^{p-1} g(\omega^j t, x),$$

where

$$g(t,x) = \sum_0^{p^{m-1}} b_k(t)x^k, \quad b_k(t) = b_k(t) = b_{k0} + b_{k1}t + \ldots + b_{k,p-1}t^{p-1} \in L(t).$$

If one coefficient b_{k1} equals 1, every $U \in \mathrm{Aut}(L(t)/K)$ with $Ut = t$ must leave $g(t,x)$ invariant since it cannot multiply t by a non-trivial power of w. Hence all the coefficients of $g(t,x)$ must belong to $K(t)$ in this case so that all the polynomials of (23) are the same and it follows that x_0 is symmetric in $t_1, \ldots, t_m$.

The situation described can be brought about by a change of the variable t to some $t' = bt^k$ according to Lemma 1. Hence we may choose $s_1, \ldots, s_m$ to be a maximal set of polynomially independent conjugates of $s' = t'^p$.

Comparison with Galois

In his article (1831a), GALOIS introduced the principles of GALOIS theory and determined the possible GALOIS group of solvable equations of prime degree, a result which we have seen is quite explicit in ABEL's article. Using this result, GALOIS deduced the general form of the GALOIS group of primitive solvable equations of primary degree p^2 (1831b). As stated above, this result was known to ABEL in another form. In contrast to the case $m = 1$, the form obtained of the GALOIS group when $m > 1$ is too general to fit all solvable equations. For instance, the group of all invertible $m \times m$ matrices mod p with determinant 1 is simple when $m > 1$. To classify all primitive solvable equations more work is needed. There is no trace of this problem in ABEL's article, but GALOIS' article (1831b) and his letter (1831c) to AUGUSTE CHEVALIER show that GALOIS' had begun thinking about this problem for the case $m = 2$.

Primitive, solvable equations after Abel and Galois

The beginnings made by ABEL and GALOIS were pursued by KRONECKER who devoted himself mainly to Abelian equations, named after ABEL's paper (1829) where it is shown that equations with commutative GALOIS groups are solvable. Equations of primary degree were treated by BETTI (1859) and Theorem 3 and Corollary 3 are given by WEBER in his book 1895, II p. 351-387.

At the time WEBER wrote his algebra, the writings of GALOIS had been understood and explained in CAMILLE JORDAN's big volume *Traité des substitutions et des équations algébriques* and ABEL's methods were forgotten. It was therefore natural for WEBER to base the theory of solvable equations on group theory.

In the first place it was then necessary for him to have our Theorem 1 cast as a property of solvable groups, *i.e.* groups G with a composition series

$$G = G_0 \supset G_{1\ldots i} \supset G_n = E$$

where every group is an invariant subgroup of prime degree in the preceding one. The property needed is that G (our $\mathrm{Aut}(L_n/K)$ of (5)) has an invariant commutative subgroup (our $\mathrm{Aut}(L_n/L_{n-1})$. WEBER's proof (1895, II pp. 33–37) is complicated when compared to the proof of Theorem 1 with a simple, direct construction of a tower of GALOIS fields from K ending in $L_n = K(f)$. The development of the theory of solvable equations would probably have been different if ABEL had written out Theorem 1 explicitly and realized its importance. The impact of GALOIS' work would then have been less in a field which it came to dominate.

In order to give the theory of primitive solvable equations of primary degree the completeness which ABEL gave to the case of prime degree, it is necessary to enumerate all possible associated towers of fields of the corresponding metacyclic groups. In many cases this was done in the framework of group theory by JORDAN (1870) and by others.

It is clear that the right side of (21) written as

$$\sum a_j(s) \sqrt[p]{s^j}.$$

produces the p^m zeros of $f(x)$ by attaching all values to the p^{th} roots of $s_1, \ldots, s_m$. Some work has been devoted to formulas for the zeros which like ABEL's formula (16), (17) involve p^{th} roots of all p^{th} powers of the resolvents or at least those in an orbit of $\mathrm{Aut}(L/K)$ where $L = L_{n-1}$. This program has been pursued by WEBER (1895, II, 383–387) when $p^m = 8$ and by WIMAN (1901), (1903), (1907) for 2^m, 3^2 and p^2, respectively. A general formula was given by BUCHT (1909). In all cases the result depends on the subgroup of $\mathrm{Aut}(L/K)$ chosen. In view of Theorem 1, it should be natural to start with the action of the primary group $\mathrm{Aut}(L_{n-1}/L_{n-2})$ where the problem is not essentially more difficult than for a cyclic group involved in (16) and (17). But then the problem is thrown back to an enumeration of the possible towers (5).

Bibliography

ABEL, N. H.
1881. *Oeuvres complètes I.II. Publiés par L. Sylow et S. Lie.*, Christiania 1881.
1824. *Mémoire les équation algébriques ou l'on démontre l'impossibilité de la résolution de l'équation générale du cinqième degré*, Christiania 1824, vol. 1 28–33.
1826a *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré*, Crelle **1** (1826) 65–84, Vol. **1**, 66–87.
1826b. *Letter to Crelle*, vol. **2**, 266.
1829. *Mémoire sur une classe particuliére d'équations résolubles algébriquement*, Crelle **4** (1829) 131–156, vol. **1**, 478–507.
1828?. *Sur la résolution algébrique des équations*, vol **2**, 217–243.
BETTI, E.
1859. *Sur la résolution par radicaux des équations dont le degre est une puissance d'un nombrepremier*, Opere I, 183–187.
BUCHT, G
1909. *Über die metazyklischen Gleichungen vom Grade p^n*, Arkiv f. Mat. Astr. Fysik bd **5** (1909) no 23.
DICKSON, L. E.
1905. *On the real elements in certain classes of geometric configurations*, Ann. Math. ser. 2, vol. **6**, no 4, 141–150.
GALOIS, E.
1831a. *Mémoire sur les conditions de résolubilité des équations par radicaux.*, Ouevres mathématiques d'Évariste Galois. Ed. Verriest Paris 1931, 33–50.
1831b. *Des équations primitives qui sont solubles par radicaux*, loc. cit. 51–59.
1831c. *Letter to Auguste Chevalier*, loc. cit. 25–32.
GÅRDING, L.
1992. *Abel and solvable equations of prime degree*, NORMAT **1**, 1992.
JORDAN, C.
1870. *Traité des substitutions et des équations algébriques*, Paris 1870.
KRONECKER, L.
1853. *Über die algebraisch auflösbaren Gleichungen*, Monatshefte Berl. Akademie (1853).
1856. *Über die algebraisch auflösbaren Gleichungen*, Monatshefte Berl. Akademie (1856).
MAILLET
1904. *Sun les équations de la geométrie et la theorie des substitutions entre n lettres*, Ann. Fac. Sc. Toulouse Sér. 2. *t. VI*, 8 (1904) 277–349.
MALMSTEN, J.
1847. *In solutionem aequationum algebraicarum disquisitio*, Crelle **34** (1847) 30–45.
SUZUKI, M.
1967 *Group Theory* I, II, Springer Grundlehren 247,248.
SYLOW, L.
1861. *Om algebraisk Oplösning af Ligninger*, Förh. Skand. Naturforsk. ottende möte, Köbenhavn 1861.
1902. *Abels studier og hans opdagelser*, Festskrift vid hundreårsjub. for Niels Henrik Abel Kristiania 1902.
VAN DER WAERDEN, B.L.
1937. *Moderne Algebra I*, Grundlehren Bd XXXIII zw. Aufl. J. Springer Berlin 1937.
WEBER, H.
1895. *Lehrbuch der Algebra in 3 Bänden*, Braunschweig: Druck und Verlag von Friedrich Vieweg und Sohn (1895–1896).
WIMAN, A.
1901a. *Über die durch Radikale auflösbaren Gleichungen deren Grad eine Potenz von 2 ist*, Öfversigt KVA Förhandlingar 1901 no 7 Stockholm.

1901b. *Über die Wurzeln der metacyklischen Gleichungen*, Öfversigt KVA Förhandlingar 1901 no 8 Stockholm.
1903. *Über die durch Radikale auflösbaren Gleichungen neunten Grades*, Arkiv Mat., Astr., Fysik bd **1** (1903–04) 665–680.
1907. *Über die metazyklischen Gleichungen vom Grade* p^2, Arkiv Mat., Astr., Fysik bd **3** nr 27 (1907).

Department of Mathematics
Lund University
22100 Lund, Sweden

and

Department of Mathematics & Statistics
University of Trondheim
7055 Dragvoll, Norway

(Received January 15, 1994)