Solvable polynomials of prime degree

February 16, 2023

Introduction

Gårding and Skau have given a modern account [5] of Abel's approach to the analysis of solvable equation. In particular, they present a proof that the degree of any primitive solvable equations has to be primary (a power of a prime number), and the general form of the root of a solvable equation of prime degree (see also [4]). This presentation however does not really follow Abel's arguments. Instead the approach there is similar to a modification of the argument already suggested by Sylow in his comments on Abel's paper [3]. Similarly, H. Edwards more recent and complete analysis of solvable equations of prime degree [6] does not follow Abel.

The goal of this note is to reconstruct Abel's argument [3], trying to understand Abel's work in terms as close to Abel's as possible, deviating thus from both Sylow and Gårding's presentations. We feel that this argument gives a better explanation of the form of the root of solvable equations of prime degree. An analysis of Abel's approach is also contained in the thesis of Sørensen [8], which refers to Sylow's comments on [3]. Sørensen has a discussion on the "highly *computation based* mathematical style of the 18th century, to which Abel had also adhered" which was marked by "lengthy, rather concrete, and painstaking algebraic manipulation". The present paper gives such a "computational" analysis of the problem of characterising solvable equation of prime degree, which can be compared with the modern account of [5]. The key Lemma is Lemma 5.1, which comes from Abel and shows that, for an irreducible solvable equation of prime degree, all roots are rational functions of the Lagrange resolvent of the equation.

1 Some Lemmas about radical extension

Let $\mathbf{L}$ be a field of characteristic 0 and q a prime number. We assume that $\mathbf{L}$ contains a primitive qth root of unity $\alpha^q = 1$ and b is an element of $\mathbf{L}$ which is not a qth power in $\mathbf{L}$. Abel proves the following results.

Lemma 1.1 *The polynomial $X^q - b$ is irreducible.*

Proof. Let P a non constant polynomial of minimal degree in $\mathbf{L}[X]$ that divides $X^q - b$. Then all polynomials $P(\alpha^i X)$ for $i = 1, \ldots, q-1$ divides also $X^q - b$ and so the polynomials $P(\alpha^i X)$ for $i = 0, \ldots, q-1$ cannot be all pairwise coprime. So they are all equal to $X^q - b$. □

The extension $\mathbf{L}[v] = \mathbf{L}[X]/\langle X^q - b\rangle$ is called a *radical* extension. The field $\mathbf{L}[v]$ is a vector space over $\mathbf{L}$ of dimension $[\mathbf{L}[v] : \mathbf{L}] = q$ and a basis is $1,\ v, \ldots,\ v^{q-1}$.

Lemma 1.2 *Let $P(X,v)$ be an irreducible polynomial in $\mathbf{L}[v][X]$ which is not in $\mathbf{L}[X]$. The polynomial*

$$Q(X) = \prod_{l=0}^{q-1} P(X, \alpha^l v)$$

is in $\mathbf{L}[X]$ and is irreducible in $\mathbf{L}[v]$. In particular, if $w = a_0 + a_1 v + \ldots + a_{q-1} v^{q-1}$ is in $\mathbf{L}[v]$ and not in $\mathbf{L}$ the minimal polynomial of w over $\mathbf{L}$ is

$$\prod_{l=0}^{q-1} (X - (a_0 + a_1 \alpha^l v + \ldots + a_{q-1} \alpha^{l(q-1)} v^{q-1}))$$

Proof. All polynomial $P(X, \alpha^i v)$ are irreducible for $i = 0, \ldots, q-1$ and they are pairwise distinct since $P(X,v)$ is not in $\mathbf{L}[X]$. If R is a non constant polynomial in $\mathbf{L}[X]$ that divides Q then R cannot be coprime to all $P(X, \alpha^i v)$, so it is divisible by one, and hence by all $P(X, \alpha^i v)$, for $i = 0, \ldots, q-1$. Since they are coprime, it is divisible by their product Q. □

Lemma 1.3 *If w is an element in $\mathbf{L}[v]$ which is not in $\mathbf{L}$ then $\mathbf{L}[w] = \mathbf{L}[v]$.*

Proof. Indeed w is of degree q over $\mathbf{L}$ by the previous Lemma. (The elements $v, 1, w, \ldots, w^{q-1}$ that can be written as $\mathbf{L}$ linear combinations of $1, v, \ldots, v^{q-1}$ have a non trivial linear relations, which gives an expression of v as a $\mathbf{L}$-linear combination of $1, w, \ldots, w^{q-1}$.) □

2 Normal and cyclic polynomials

If g is a irreducible polynomial over $\mathbf{K}$ of degree m, we can consider the extension $\mathbf{K}[r] = \mathbf{K}[X]/\langle g \rangle$ where we add formally one root r of g. We say that g is a *normal* polynomial iff g has m roots $r,\ r_1,\ \ldots,\ r_{m-1}$ in $\mathbf{K}[r]$. In such a situation, we can define the maps $h(r) \longmapsto h(r_i)$, which are automorphisms of $\mathbf{K}[r]$ for $i = 0,\ \ldots,\ m-1$. (The construction of similar automorphisms plays a crucial role in the paper [2], and of course, in Galois' presentation of his theory, and this is where the notion of irreducibility appears.) If $s = h(r)$ is an element of $\mathbf{K}[r]$ the *conjugates* of s are the elements $s,\ s_1 = h(r_1),\ \ldots,\ s_{m-1} = h(r_{m-1})$. If these elements are all distinct then we have $\mathbf{K}[s] = \mathbf{K}[r]$. Indeed, if q is in $\mathbf{K}[X]$ and $q(s) = 0$ then $q(h(r)) = 0$ and so $q(h(r_i)) = 0$ for $i = 0,\ 1,\ \ldots,\ m-1$. It follows that the minimal polynomial of s over $\mathbf{K}$ is

$$\prod_{l=0}^{m-1} (X - s_l)$$

If θ is the automorphism $h(r) \longmapsto h(r_1)$ then $\theta(r)$ is a root of g, and so are $\theta^2(r),\ \theta^3(r),\ \ldots$ In the case where this enumerates all roots of h, that is, when all $r,\ \theta(r),\ \ldots,\ \theta^{m-1}(r)$ are distinct, we say that g is a *cyclic* polynomial. (Abel shows in [2] that a cyclic polynomial is solvable.)

3 Lagrange resolvent

Let $\mathbf{k}$ be a field and $\mathbf{K} = \mathbf{k}[\alpha]$ the extension of $\mathbf{k}$ by a primitive p-root of unity $\alpha^p = 1$, where p is a prime number. (We can have $\mathbf{K} = \mathbf{k}$ if $\mathbf{k}$ contains already a primitive p-root of unity.)

If $\sigma \in \mathfrak{S}_p$ is a permutation of $0, \ldots, p-1$ we define

$$u_\sigma = \frac{1}{p} \sum_{l=0}^{p-1} \alpha^{-l} X_{\sigma(l)}$$

This is a polynomial in $\mathbf{K}[X_0, \ldots, X_{p-1}]$. We shall see that Abel's analysis of solvable equations explains in a natural way why considering this element, the *Lagrange resolvent*.

We write $S_0, \ldots, S_{p-1}$ the elementary symmetric polynomials in $X_0, \ldots, X_{p-1}$

$$S_0 = X_0 + \ldots + X_{p-1} \quad \ldots \quad S_{p-1} = X_0 \ldots X_{p-1}$$

Lemma 3.1 *If R is a polynomial in $\mathbf{k}[X]$ the element*

$$p_l = \sum_{\sigma \in \mathfrak{S}_p} R(u_\sigma) X_{\sigma(l)}$$

is in $\mathbf{K}[S_0, \ldots, S_{p-1}]$, and the element p_0 is in $\mathbf{k}[S_0, \ldots, S_{p-1}]$.

Proof. It is clear that p_l is a symmetric polynomial in $X_0, \ldots, X_{p-1}$ and hence it belongs to $\mathbf{k}[\alpha, S_0, \ldots, S_{p-1}]$. Furthermore, p_0 is invariant by the change of α to α^i for $i = 1, \ldots, p-1$ and hence p_0 is in $\mathbf{k}[S_0, \ldots, S_{p-1}]$. □

4 Solvable equations

Let $\mathbf{k}$ be a field of characteristic 0 and $\mathbf{K}$ the extension of $\mathbf{k}$ obtained by adding all roots of unity. We consider a polynomial equation $f(x) = 0$ over $\mathbf{k}$. We say that this equation is *solvable* iff there exists a sequence of radical extensions

$$\mathbf{K}_1 = \mathbf{K}[u_1],\ \mathbf{K}_2 = \mathbf{K}_1[u_2],\ \ldots,\ \mathbf{K}_n = \mathbf{K}_{n-1}[u_n]$$

$$u_1^{p_1} \in \mathbf{K},\ u_2^{p_2} \in \mathbf{K}[u_1],\ \ldots\ , u_n^{p_n} \in \mathbf{K}[u_1, \ldots, u_{n-1}]$$

with $p_1, \ldots, p_n$ prime and u_{i+1} not in $\mathbf{K}_i = \mathbf{K}[u_1, \ldots, u_i]$ such that f has a root x_0 in $\mathbf{K}_n$.

$\mathbf{K}_{i+1}$ is a vector space over $\mathbf{K}_i$ of dimension $[\mathbf{K}_{i+1} : \mathbf{K}_i] = p_i$ and the dimension of $\mathbf{K}_n$ over $\mathbf{K}$ is $[\mathbf{K}_n : \mathbf{K}] = p_n \ldots p_1$.

Notice that we have an explicit basis of $\mathbf{K}_n$ over $\mathbf{K}$ which is given by all monomials

$$u_1^{i_1}\ \ldots\ u_n^{i_n}$$

with $i_1 < p_1,\ \ldots,\ i_n < p_n$.

We have an element x_0 in $\mathbf{K}_n$ such that $f(x_0) = 0$. If x_0 is already in $\mathbf{K}_{n-1}$ we can shorten the sequence $u_1, \ldots, u_n$. In this way, we can assume that x_0 is in $\mathbf{K}_n$ but not in $\mathbf{K}_{n-1}$.

We can write

$$x_0 = q_0 + q_1 u_n + q_2 u_n^2 + \ldots + q_{p_n - 1} u_n^{p_n - 1}$$

with $q_0, q_1, \ldots$ in $\mathbf{K}_{n-1}$. Since x_0 is not in $\mathbf{K}_{n-1}$, some of the term $q_1,\ q_2,\ \ldots$ is $\neq 0$. We have $\mathbf{K}_{n-1}[u_n] = \mathbf{K}_{n-1}[q_l u_n^l]$ by Lemma 1.3 if $q_l \neq 0$. Let us write $w = q_l u_n^l$. Since w^{p_n} is in $\mathbf{K}_{n-1}$, and not in $\mathbf{K}_{n-1}$, we can write

$$x_0 = c_0 + c_1 w + c_2 w^2 + \ldots + c_{p_n - 1} w^{p_n - 1}$$

The equality

$$c_0 + c_1 w + c_2 w^2 + \ldots + c_{p_n - 1} w^{p_n - 1} = q_0 + q_1 u_n + q_2 u_n^2 + \ldots + q_{p_n - 1} u_n^{p_n - 1}$$

shows, by comparing the coefficient of u_n^l in both expressions, that we have $c_1 = 1$. Thus, by replacing u_n by $q_l u_n^l$, we can thus assume that we can write

$$x_0 = q_0 + u_n + q_2 u_n^2 + \ldots + q_{p_n - 1} u_n^{p_n - 1}$$

5 Solvable equations of prime degree

Assume now that the equation $f(x) = 0$ is monic, irreducible and of prime degree p. Abel proves in this case that $p_n = p$ in the following way.

Since $\mathbf{K}_{n-1}[x_0] = \mathbf{K}_n$ the minimal polynomial of x_0 over $\mathbf{K}_{n-1}$ is by Lemma 1.2

$$\prod_{l=0}^{p-1}(X - (q_0 + \alpha_n^l u_n + q_2\alpha_n^{2l}u_n^2 + \ldots + \alpha_n^{(p_n-1)l}q_{p_n-1}u_n^{p_n-1}))$$

with $\alpha_n^{p_n} = 1$.

This polynomial is in $\mathbf{K}_{n-1}[X]$. We take $i_1 < n$ minimal such that it can be written in $\mathbf{K}_{i_1}[X]$. Being irreducible in $\mathbf{K}_{n-1}[X]$ this polynomial is irreducible in $\mathbf{K}_{i_1}[X]$ as well, and can be written $Q(X, u_{i_1})$ with coefficients in $\mathbf{K}_{i_1-1}$. The polynomial

$$\prod_{l=0}^{p_{i_1}-1} Q(X, \alpha_{i_1}^l u_{i_1})$$

is irreducible in $\mathbf{K}_{i_1-1}[X]$ by Lemma 1.2 and is in $\mathbf{K}_{i_2}[X]$ for some $i_2 < i_1$, and of degree $p_n p_{i_1}$. In this way, one shows that the degree of the minimal polynomial of x_0 over $\mathbf{K}$ has to be of the form $p_n p_{i_1} p_{i_2} \ldots$. But since $f(x_0) = 0$ and f is irreducible of degree p one should have $p = p_n p_{i_1} p_{i_2} \ldots$. Since p is prime this is only possible if $p_n = p$ and

$$f(X) = \prod_{l=0}^{p-1}(X - (q_0 + \alpha_n^l u_n + q_2\alpha_n^{2l}u_n^2 + \ldots + \alpha_n^{(p_n-1)l}q_{p_n-1}u_n^{p_n-1}))$$

We write $\alpha = \alpha_n$ and $u = u_n$. In $\mathbf{K}_n$ the polynomial f has p roots

$$x_l = q_0 + \alpha^l u + q_2\alpha^{2l}u^2 + \ldots + q_{p-1}\alpha^{(p-1)l}u^{p-1}$$

for $l = 0, \ldots, p-1$. It follows that we have

$$u = \frac{1}{p}(x_0 + \alpha^{-1}x_1 + \ldots + \alpha^{-(p-1)}x_{p-1})$$

We see that u is in $\mathbf{k}[\alpha, x_0, \ldots, x_{p-1}]$. The element u is the (Lagrange) *resolvent* of the equation $f(x) = 0$. We see that Abel's analysis explains where this resolvent comes from. We follow now Abel in showing that $x_0, \ldots, x_{p-1}$ are in $\mathbf{k}[\alpha, u]$, so that $\mathbf{k}[\alpha, u] = \mathbf{k}[\alpha, x_0, \ldots, x_{p-1}]$ and x_0 is in $\mathbf{k}[u]$.

If $\sigma \in \mathfrak{S}_p$ is a permutation of $0, \ldots, p-1$ we define

$$u_\sigma = \frac{1}{p}\sum_{l=0}^{p-1} \alpha^{-l}x_{\sigma(l)}$$

5.1 All roots are rational functions of the resolvent

We follow Abel, contrary to Netto [7], who uses Galois theory at this point. The polynomial

$$P(X) = \prod_{\sigma\in\mathfrak{S}_p}(X - u_\sigma)$$

is in $\mathbf{k}[X]$ and such that $P(u) = 0$. If $R = P/(X-u)$ we have R in $\mathbf{k}[u][X]$ and we claim that $R(u) \neq 0$.

Lemma 5.1 *If $u_\sigma = u$ then $\sigma(l) = l$ for all l.*

Proof. Assume $u_\sigma = u$. This can be written as

$$u = \frac{1}{p}\sum_{l=0}^{p-1} \alpha^{-l} x_{\sigma(l)} = \frac{1}{p}\sum_{l=0}^{p-1} \alpha^{-l}(q_0 + \alpha^{\sigma(l)}u + q_2\alpha^{2\sigma(l)}u^2 + \ldots + q_{p-1}\alpha^{(p-1)\sigma(l)}u^{p-1})$$

with $q_0, q_2, \ldots, q_{p-1}$ in $\mathbf{K}_{n-1}$ and hence, comparing the coefficient of u in both side of this equality

$$1 = \frac{1}{p}\sum_{l=0}^{p-1} \alpha^{-l}\alpha^{\sigma(l)}$$

or

$$p = \sum_{l=0}^{p-1} \alpha^{-l}\alpha^{\sigma(l)}$$

This equality is only possible if $\sigma(l) = l$ for all l. □

By Lemma 3.1, the element

$$R(u)x_l = \sum_{\sigma\in\mathfrak{S}_p} R(u_\sigma)x_{\sigma(l)}$$

is in $\mathbf{k}[\alpha]$, since it is symmetric in $x_0, \ldots, x_{p-1}$. Furthermore, also by Lemma 3.1, the element $R(u)x_0$ is in $\mathbf{k}$.

Corollary 5.2 $\mathbf{k}[\alpha, u] = \mathbf{k}[\alpha, x_0, \ldots, x_{n-1}]$ *and* x_0 *is in* $\mathbf{k}[u]$.

We can write

$$x_l = q_0(v) + \omega^l u + q_2(v)\omega^{2l}u^2 + \ldots + q_{p-1}(v)\omega^{(p-1)l}u^{p-1}$$

with q_j in $\mathbf{k}[X]$ and $v = u^p$.

Since

$$q_0(v) = \frac{1}{p}(x_0 + \ldots + x_{p-1})$$

we see that $q_0(v) = q_0$ is in $\mathbf{k}$.

We write $\Omega = \mathbf{k}[\alpha, u] = \mathbf{k}[\alpha, x_0, \ldots, x_{n-1}]$. In modern term, Ω is a *normal* extension of $\mathbf{k}$. Abel's analysis consists precisely in looking at all conjugates of u in Ω and expressing that

$$x_0 = q_0 + u + q_2(v)u^2 + \ldots + q_{p-1}(v)u^{p-1}$$

has only p conjugates.

5.2 The conjugates of the resolvent

The root of the minimal polynomial F of u over $\mathbf{K}$ are called the *conjugates* of u. They are all in Ω, since they are among the elements $u_\sigma,\ \sigma \in \mathfrak{S}_p$ and $x_0,\ x_1,\ \ldots,\ x_{p-1}$ are in $\mathbf{k}[\alpha, u]$.

If u' is a conjugate of u we define an automorphism of Ω by extending the map $\mathbf{k}[u] \to \Omega,\ r(u) \longmapsto r(u')$ to Ω. For extending this map, we look at the minimal polynomial $Q(X, u)$ of α and we choose a root α' of $Q(X, u')$. The conditions $\varphi(u) = u'$ and $\varphi(\alpha) = \alpha'$ defines then an automorphism of Ω. All automorphisms of $\Omega/\mathbf{k}$ can be obtained in this way and we get a complete description of the elements of the group H of automorphisms of the extension $\Omega/\mathbf{k}$.

Via an automorphism $u \longmapsto u',\ \alpha \longmapsto \alpha'$, the element $v = u^p$ is sent to the element $v' = u'^p$. I claim that we have $\mathbf{k}[\alpha, v] = \mathbf{k}[\alpha, v']$. Indeed, if v' is not in $\mathbf{k}[\alpha, v]$ we have by Lemma 1.3, $\mathbf{k}[\alpha, v'] = \Omega$, since Ω is a radical extension of $\mathbf{k}[\alpha, v]$, and this contradicts that u' is not in $\mathbf{k}[\alpha, v']$.[1].

Let G the minimal polynomial of v over $\mathbf{k}$. We have $F(X) = G(X^p)$. We are going to see that the degree ν of G divides $p-1$. Furthermore, there is a polynomial θ in $\mathbf{k}[X]$ such that the roots of G are exactly the element $v,\ \theta(v),\ \ldots,\ \theta^{\nu-1}(v)$.

Since u' is in $\Omega = \mathbf{k}[\alpha, u]$ we can write

$$u' = c_0 + c_1 u + \ldots + c_{p-1} u^{p-1}$$

with $c_0, \ldots, c_{p-1}$ in $\mathbf{k}[\alpha, v]$. Since u'^p is in $\mathbf{k}[\alpha, v'] = \mathbf{k}[\alpha, v]$ we have by Lemma 1.2 a relation of the form

$$\alpha u' = c_0 + c_1 \alpha^j u + \ldots + c_{p-1} \alpha^{j(p-1)} u^{p-1}$$

and so

$$\alpha c_0 + c_1 \alpha u + \ldots + c_{p-1} \alpha u^{p-1} = c_0 + c_1 \alpha^j u + \ldots + c_{p-1} \alpha^{j(p-1)} u^{p-1}$$

It follows that $c_i = 0$ if $i \neq l$ and u' is necessarily of the form $c_l u^l$ with $jl = 1$ mod. p.

Since we have $f(x_0) = 0$ where

$$x_0 = q_0 + u + q_2(v) u^2 + \ldots + q_{p-1}(v) u^{p-1}$$

it follows that

$$q_0 + u' + q_2(v') u'^2 + \ldots + q_{p-1}(v') u'^{p-1}$$

is also a root of f and so we have for some k

$$q_0 + u' + q_2(v') u'^2 + \ldots + q_{p-1}(v') u'^{p-1} = q_0 + \alpha^k u + q_2(v) \alpha^{2k} u^2 + \ldots + q_{p-1}(v) \alpha^{k(p-1)} u^{p-1}$$

and since $\mathbf{k}[\alpha, v'] = \mathbf{k}[\alpha, v]$ and $u' = c_l u^l$ it follows that we have $c_l = q_l(v) \alpha^{kl}$.

In conclusion, the roots of f can be written

$$x_i = q_0 + \alpha^i u + q_2(v) \alpha^{2i} u^2 + \ldots + q_{p-1}(v) \alpha^{i(p-1)} u^{p-1}$$

and the conjugates of u are necessarily of the form $q_l(v) u^l \alpha^j$.

Notice that if $\varphi(u) = q_l(v) u^l \alpha^j$ then we have $\varphi(x_0) = x_k$ such that $lk = j$ mod. p.

Any automorphism φ of $\Omega/\mathbf{k}$ necessarily sends u to an element of the form $\varphi(u) = q_l(v) u^l \alpha^j$. If we have another automorphism ψ which sends u to an element $\psi(u) = q_t(v) u^t \alpha^k$, the element $\psi(\varphi(u))$ has to be of the form $q_s(v) u^s \alpha^l$ and s is the product lt modulo p.

We thus have a group morphism $H \to (\mathbb{Z}/p\mathbb{Z})^\times$ of the group of automorphism of $\Omega/\mathbf{k}$ into the multiplicative group of the nonzero elements mod. p. Let g be a primitive root modulo p and choose $k = g^l$ mod. p which generates the image of this morphism. We know that l divides $p-1$ and we write $l\nu = p-1$. We have

$$\theta(u) = q_k(v) u^k \alpha^j$$

and we can assume $j = 0$ since the conjugates of u are closed under multiplication by α. (We have used only in a superficial way the modern notion of group of automorphisms to simplify the exposition, but all these last steps were clear to Abel.)

[1]This is the step which is not completely clear in either Netto or Abel [3, 7]. Sylow suggests a modification of Abel's argument, which is followed in [5], involving normal closures.

We know that $\theta(x_0)$ is a root of the polynomial f. Also, since $\theta(u) = q_k(v)u^k\omega^0$ we have necessarily $\theta(x_0) = x_0$. We have then

$$\theta^2(u) = q_{k_2}(v)u^{k_2},\ \theta^3(u) = q_{k_3}(v)u^{k_3},\ \ldots$$

with $k^n = k_n$ mod. p.

The conjugates of u are then exactly the elements $q_{k_n}(v)u^{k_n}\alpha^i$. Hence u has exactly $p\nu$ conjugates and ν is the degree of v.

We have

$$\theta(v) = \theta(u^p) = q_k(v)^p v^k$$

and the conjugates of v are $\theta(v),\ \theta^2(v),\ \ldots,\ \theta^{\nu-1}(v)$ and $\theta^\nu(v) = v$. We see that v is the root of a *cyclic polynomial* of degree ν which divides $p-1$.

Let us write (i) for g^{il}. We can write $\theta(u) = hu^{(1)}$ and h in $\mathbf{k}[v]$ has for conjugates $h = h_0,\ h_1,\ \ldots,\ h_{\nu-1}$. We then have

$$\theta^2(u) = \theta(h)(\theta(u))^{(1)} = h_1 h_0^{(1)} u^{(2)}$$

and more generally

$$\theta(u) = hu^{(1)},\ \theta^2(u) = h_1 h_0^{(1)} u^{(2)},\ \ldots,\ \theta^\nu(u) = u = h_{\nu-1}h_{\nu-2}^{(1)}\ldots h_0^{(\nu-1)}u^{(\nu)}$$

We can choose g such that $(\nu) - 1 = np$ and n is *not* divisible by p: if $g^{p-1} - 1$ is divisible by p^2, then $(g+p)^{p-1} - 1$ is not divisible by p^2 and we can change g to $g+p$. We have

$$1 = h_{\nu-1}h_{\nu-2}^{(1)}\ldots h_0^{(\nu-1)}v^n$$

and we can then find t and s such that $nt + 1 = ps$, so that

$$v = (v^s)^p r_{\nu-1}^{(0)} r_{\nu-2}^{(1)} \ldots r_0^{(\nu-1)}$$

with $r = h_0^t$. The elements $r = r_0,\ r_1,\ \ldots,\ r_{\nu-1}$ have to be pairwise distinct since v is not of pth power in $\mathbf{k}[\alpha, v]$. It follows[2] that we have $\mathbf{k}[r_0] = \mathbf{k}[v]$ and so we can write $v^s = \psi(r)$. Also the element $w = u/\psi(r)$ satisfies

$$w^p = r_{\nu-1}^{(0)} r_{\nu-2}^{(1)} \ldots r_0^{(\nu-1)}$$

We have

$$v = \psi(r_0)^p\ \ r_{\nu-1}^{(0)} r_{\nu-2}^{(1)} \ldots r_0^{(\nu-1)} \qquad \ldots \qquad v_{\nu-1} = \psi(r_{\nu-1})^p\ \ r_{\nu-2}^{(0)} r_{\nu-3}^{(1)} \ldots r_{\nu-1}^{(\nu-1)}$$

6 Summary of the analysis

In order to build the roots of a solvable irreducible polynomial of prime degree p, we take a divisor ν of $p-1$ and a cyclic polynomial of degree ν with roots $r = r_0,\ r_1,\ \ldots,\ r_{\nu-1}$. We assume that $p - 1 = l\nu$. We choose a primitive root g mod. p. We consider the elements, where (i) denotes g^{li}

$$s = r_0^{(\nu-1)} r_1^{(\nu-2)} \ldots r_{\nu-1}^{(0)}\ \ s_1 = r_1^{(\nu-1)} r_2^{(\nu-2)} \ldots r_0^{(\nu-1)} \quad \ldots \quad s_{\nu-1} = r_{\nu-1}^{(\nu-1)} r_0^{(\nu-2)} \ldots r_{\nu-2}^{(\nu-1)}$$

[2]Netto does not observe that we must have $\mathbf{k}[v] = \mathbf{k}[r]$ but states this as an extra hypothesis. On the contrary, Sylow in his analysis of Abel's paper [3], states that it is easy to see, "on voit facilement", that r is of degree ν over $\mathbf{k}$.

We assume that the element s is not a pth power in $\mathbf{K}[r]$ so that the radical extension $\mathbf{K}[w]$ with $w^p = s$ is of degree p over $\mathbf{K}[r]$. We write $(\nu) - 1 = np$ and we define $w_1 = w^{(1)}/r_0^n$ so that $w_1^p = s_1$ and

$$w_2 = w_1^{(1)}/r_1^n = w^{(2)}/r_0^{n(1)} r_1^n,\ w_3 = w_2^{(1)}/r_2^n = w^{(3)}/r_0^{n(2)} r_1^{n(1)} r_2^n,\ \ldots$$

and we have

$$w_{\nu-1}^{(1)}/r_{\nu-1}^n = w w^{np}/s^n = w$$

The elements $w,\ w_1,\ \ldots,\ w_{\nu-1}$ are linearly independent over $\mathbf{K}[r]$ since v is not a pth power in $\mathbf{K}[r]$ by hypothesis. (It follows from this that the elements $s,\ s_1,\ \ldots,\ s_{\nu-1}$ are pairwise distinct and that s is of degree ν over $\mathbf{K}$.) The elements

$$x_0 = q_0 + \sum_{i=0}^{\nu-1} \psi_0(r_i) w_i + \sum_{i=0}^{\nu-1} \psi_1(r_i) w_i^g + \ldots + \sum_{i=0}^{\nu-1} \psi_{l-1}(r_i) w_i^{g^{l-1}}$$

have exactly p conjugates (provided we have $\psi_j(r) \neq 0$ for some j).

Furthermore, any solvable polynomial of degree p can be obtained in this way.

Notice that we don't require that n is not divisible by p.

7 Example: solvable equations of degree 5

7.1 Case $\nu = 1$

We take an arbitrary v in $\mathbf{K}$ which is not a 5th power and the general form of the root is

$$q_0 + u + \psi_1 u^2 + \psi_2 u^4 + \psi_3 u^3$$

with q_0 in $\mathbf{K}$, and $\psi_1,\ \psi_2,\ \psi_3$ in $\mathbf{K}$ and $u^5 = v$.

7.2 Case $\nu = 2$

We take a cyclic polynomial of degree 2 and root $r,\ r_1$ such that $r^4 r_1$ is not a 5th power in $\mathbf{K}[r]$. Then if we consider the radical extension $w^5 = r^4 r_1$ and $w_1 = w^4/r^3$, so that $w_1^5 = r_1^4 r$. For any polynomials ψ_0 and ψ_1 the element

$$x_0 = q_0 + \psi_0(r) w + \psi_0(r_1) w_1 + \psi_1(r) w^2 + \psi_1(r_1) w_1^2$$

has 5 conjugates (provided $\psi_0(r) \neq 0$ or $\psi_1(r) \neq 0$). On the other hand the element w has 10 conjugates of the form $\alpha^i w$ and $\alpha^i w_1$. If w is sent to $\alpha^i w$ then $w^5 = r^4 r_1$ is not modified, so that r is sent to r and $w_1 = w^4/r^3$ is sent to $\alpha^{4i} w_1$ and x_0 is sent to

$$x_i = q_0 + \psi_0(r) \alpha^i w + \psi_0(r_1) \alpha^{4i} w_1 + \psi_1(r) \alpha^{2i} w^2 + \psi_1(r_1) \alpha^{3i} w_1^2$$

On the other hand, if w is sent to $\alpha^i w_1$ then r is sent to r_1 and x_0 is sent to

$$x_{4i} = q_0 + \psi_0(r_1) \alpha^i w_1 + \psi_0(r) \alpha^{4i} w + \psi_1(r_1) \alpha^{2i} w_1^2 + \psi_1(r) \alpha^{3i} w^2$$

7.3 Case $\nu = 4$

We take a cyclic polynomial of degree 4 and root $r,\ r_1,\ r_2,\ r_3$ such that $r^8 r_1^4 r_2^2 r_3$ is not a 5th power in $\mathbf{K}[r]$. We consider the radical extension $w^5 = r^8 r_1^4 r_2^2 r_3$ and

$$w_1 = w^2/r^3,\ w_2 = w^4/r^6 r_1^3,\ w_3 = w^8/r^{12} r_1^6 r_2^3$$

Then for any $\psi(r) \neq 0$ the element

$$x_0 = q_0 + \psi(r)w + \psi(r_1)w_1 + \psi(r_2)w_2 + \psi(r_3)w_3$$

is of degree 5 over $\mathbf{K}$.

There is in the reference [9] an analysis of the form of the general cyclic equation of degree 4.

Notice that, in his letter to Crelle where Abel gives the general form of solvable equations of degree 5, Abel seems to limit himself to the case $\nu = 4$. Similarly, Kronecker, in his 1853 note (where he announced what is now known as the Kronecker-Weber theorem), seems to limit himself to the case where $\nu = p - 1$. (This is pointed out in the reference [6].)

8 Primitive solvable polynomials

Abel's paper [3] goes further than the analysis of solvable irreducible equations of prime degree. This is explained in [4, 5], using however Galois theory in an essential way. We think that the main idea can be explained without using Galois theory, following Sylow's explanations of Abel's paper. This consists in organising the sequence of radical extensions

$$\mathbf{K},\ \mathbf{K}[u_1],\ \mathbf{K}[u_1, u_2],\ \ldots$$

in a special way. (This way appears in some drafts of Abel, according to Sylow.) First, we don't assume anymore that $\mathbf{K}$ contains all roots of unity and we start from the base field $\mathbf{k}$, adding roots of unity when needed. Second, at each stage, we have a normal extension $\mathbf{K}$ of $\mathbf{k}$ with a complete description of all automorphisms of $\mathbf{K}/\mathbf{k}$. For the next stage, instead of adding only one root of $X^p - a$ if a is in $\mathbf{K}$ is not a pth power, we add first a primitive p-root of unity $\alpha^p = 1$ (if necessary) and then we add a root for *each* polynomial $X^p - a'$ where a' is a conjugate of a over k. We thus obtain an extension

$$\mathbf{L} = \mathbf{K}[\alpha, u_1, \ldots, u_m]$$

of $\mathbf{K}[\alpha]$ of degree p^m for some m with $u_i^m = a_i$ in $\mathbf{K}$ is a conjugate of a. We still have a complete description of the automorphisms of $\mathbf{L}/\mathbf{k}$. Given any automorphism φ of $\mathbf{K}/\mathbf{k}$, we explain how to extend it to an automorphism of $\mathbf{L}/\mathbf{k}$. First we have to choose $\varphi(\alpha) = \alpha'$. There are as many choices as the degree of α over $\mathbf{K}$. Then we choose a root u_1' in $\mathbf{L}$ of $X^p - \varphi(a_1)$. The polynomial $X^p - \varphi(a_2)$ as no root in $\mathbf{K}[\alpha', u_1']$, since $X^p - a_2$ as no root in $\mathbf{K}[\alpha, u_1]$. We choose a root u_2' in $\mathbf{L}$ of $X^p - \varphi(a_2)$. We define in this way $\varphi(u_1) = u_1',\ \varphi(u_2) = u_2', \ldots$

As noted in [5], the group of automorphisms of the extension $\mathbf{L}/\mathbf{K}[\alpha]$ is commutative and isomorphic to $(\mathbb{Z}/p\mathbb{Z})^m$.

References

[1] N.H. Abel Mémoire sur les équations algébriques où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré Christiana, 1824.

[2] N.H. Abel Mémoire sur une classe particulière d'équations résolubles algébriquement. J. reine angew. Math. 4, 131-156, 1829.

[3] N.H. Abel Sur la résolution algébrique des équations. Oeuvres complètes.

[4] L. Gårding. Abel och lösbara ekvationer av primtalsgrad. Normat 1, 1992.

[5] L. Gårding and Ch. Skau. Niels Henrik Abel and Solvable Equations. Archive for History of Exact Sciences, 1994, 81-103.

[6] H. Edwards. The construction of solvable polynomials. BAMS, 2009, 397-411.

[7] E. Netto. *Theory of substitutions.* Wahr, Ann Arbor 1892. (Chelsea reprint, 1964.)

[8] H.K. Sørensen. *Niels Henrik Abel and the theory of equations.* Appendix of progress report, Institut for Videnskabshistorie, Aarhus Universitet, Aarhus, 1999.

[9] M.H. Vogt. *Lecons sur la résolution algébrique des équations.* Paris, Nony, 1895.