Solvable polynomials of prime degree

January 27, 2012

Introduction

As stressed by H. Edwards [6, 7], Kronecker's approach to the resolution of equation [8] differs from the one of Galois. Inspired by Abel's work [3], he stated the problem, of finding *all polynomials that are solved by radicals*, while Galois aims at *characterizing* which polynomials are solved by radicals. Kronecker 1953 paper [8], well-known for containing the statement of Kronecker-Weber's Theorem, emphasizes this difference. Following Abel, Kronecker sketches a possible solution for irreducible equations of prime degree. The main ideas of this solution seem to be already present in Abel's work [3][1].

Surprisingly, given the importance of Kronecker's problem, few works address this question of finding all solvable polynomials. Possible references are the works of Abel [3], corrected by Sylow, and its modern account by Gårding and Skau [5], or its more traditional account by Netto [10] or the thesis of Sørensen [11]. But all these works assume (sometimes only in an implicit way) that the base fields contain all roots of unity. This is not satisfactory if one wants to describe for instance all solvable equations over the field of rationals. Only H. Edwards' work [6, 7] and Sylow's presentation of Abel's paper [3] are careful about this point and presents a general solution in the case of irreducible equation of prime degree over a general base field.

The goal of this paper is to present an elementary solution of Kronecker's problem, which refines in some sense Edwards' solution, and follows very closely Abel's arguments [3]. Following [6] (and Kronecker) we work only with "algebraic field", so that we can always explicitely find a decomposition of a polynomial in irreducible factors over these fields.

1 Solvable polynomials

Let $\mathbf{k}$ be a field of characteristic 0 and P a polynomial in $\mathbf{k}[X]$. We say that P is *solvable* iff there exists a sequence of radical extensions $\mathbf{k}_1 = \mathbf{k}[u_1],\ \mathbf{k}_2 = \mathbf{k}[u_1, u_2], \ldots,\ \mathbf{k}_n = \mathbf{k}[u_1, \ldots, u_n]$ such that P has a root in $\mathbf{k}_n$. A *radical extension* of a field $\mathbf{k}$ is of the form $\mathbf{k}[u] = \mathbf{k}[X]/\langle X^p - v\rangle$ where p is prime and v an element in $\mathbf{k}$ which is not a pth power in $\mathbf{k}$.

Lemma 1.1 *If v in $\mathbf{k}$ is not a pth power in $\mathbf{k}$ then the polynomial $X^p - v$ is irreducible.*

Proof. Abel [3] proved this result assuming that $\mathbf{k}$ contains a primitive pth root of unity. We follow the proof in [10]: if f is a monic polynomial of degree l which divides $X^p - v$ then all roots u of f satisfy $u^p = v$ and so $f(0)^p$, which is $(-1)^l$ times the product of all u^p, is equal to $(-1)^l v^l$. If $l < p$ then l and p are coprime and this implies that v is in $\mathbf{k}^p$. □

Using this lemma, we see that $\mathbf{k}[X]/\langle X^p - v\rangle$ is indeed a field extension of $\mathbf{k}$.

2 Analysis of solvable equations of prime degree

Let p be a prime number.

The goal is to generate all irreducible solvable polynomials P in $\mathbf{k}[X]$ of degree p. In this section we analyse this goal starting from the following result, that we shall prove in the next section using more

[1] As suggested in [5], it seems that Kronecker knew about Abel's work only through Malmstem [9] presentation.

or less exactly Abel's arguments [3]. We start by taking an irreducible factor of $X^{p-1}+\ldots+X+1$ and consider $\mathbf{K}$ the extension of $\mathbf{k}$ with a root of this factor. We have $\mathbf{K}=\mathbf{k}[\alpha]$ with $\alpha^p=1$ a primitive pth root of unity, but we can have $\mathbf{K}=\mathbf{k}$ if $\mathbf{k}$ contains already a primitive pth root of unity α.

Theorem 2.1 *If P is solvable it is possible to build the splitting field $\Omega=\mathbf{K}[x_0,\ldots,x_{p-1}]$ of P in such a way that if we define*

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

and $v=u^p$, we have $\Omega=\mathbf{K}[u]$. Furthermore, we can find q_0 in $\mathbf{k}$ and $q_2,\ldots,q_{p-1}$ in $\mathbf{k}[v]$ such that

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

for $i=0,\ldots,p-1$ and the element u is not in $\mathbf{K}[v]$.

As we are going to see, it is possible to deduce from this by elementary arguments the structure of solvable irreducible polynomials of degree p. We don't use any Galois theory, though the argument can be seen as a motivation of Galois theory. On the other hand, we use the structure of cyclic extensions as analysed by Abel [2].

Abel's key idea [3] consists in looking at the possible "conjugates" of u over $\mathbf{k}$, or, what amounts to the same, the possible morphism $\mathbf{k}[u]\to\Omega$ and expressing that when we change u by one of its conjugate in the expression

$$x_0=q_0+u+q_2u^2+\ldots+q_{p-1}u^{p-1}$$

then x_0 has to become another root x_i of the polynomial P.

2.1 First analysis

Before analysing the conjugates of u we notice that, since $\Omega=\mathbf{K}[x_0,\ldots,x_{p-1}]=\mathbf{K}[u]$ and $\mathbf{K}=\mathbf{k}[\alpha]$ the degree of the extension $\Omega/\mathbf{k}$ is of the form pm where m is a product of numbers $<p$ and hence p does not divide m. Since u is of degree p over $\mathbf{K}[v]$, it follows from this that the degree of v over $\mathbf{k}$ is not divisible by p. Since $\Omega=\mathbf{K}[x_0,\ldots,x_{p-1}]=\mathbf{K}[u]$ the element u is a root of a polynomial in $\mathbf{k}[X]$ that is linearly factored in Ω. To give a morphism $\varphi:\mathbf{k}[u]\to\Omega$ is the same as to give a conjugate of u in Ω that is a root of the minimal polynomial of u over $\mathbf{k}$. The number of such morphisms is thus equal to the degree of u over $\mathbf{k}$.

We now look at a morphism $\varphi:\mathbf{k}[u]\to\Omega$. Following Abel, we write $u'=\varphi(u),\ v'=\varphi(v)=u'^p$. The degree of v' over $\mathbf{k}$ is the same as the one of v and hence is not divisible by p. It follows that we have v' in $\mathbf{K}[v]$, otherwise we would have $\mathbf{K}[v,v']=\mathbf{k}[\alpha,v,v']=\Omega$, which is not possible since the degree of Ω over $\mathbf{k}$ is divisible by p. So we have $\varphi(v)$ in $\mathbf{K}[v]$. Since u' is in $\Omega=\mathbf{K}[u]$ we can write

$$u'=c_0+c_1u+\ldots+c_{p-1}u^{p-1}$$

with $c_0,\ldots,c_{p-1}$ in $\mathbf{K}[v]$. Since v' is in $\mathbf{K}[v]$ and u is of degree p over $\mathbf{K}[v]$ the equation $X^p=v'$ has for solutions

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

and since $\alpha u'$ is also a solution of this equation, we should have an equality 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_lu^l where l is such that $jl=1$ mod. p.

Since we have $P(x_0)=0$ 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 P 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 $\mathbf{K}[v'] = \mathbf{K}[v]$ and $u' = c_l u^l$ it follows that we have $c_l = q_l(v)\alpha^{kl}$.

In conclusion, the conjugates of u are necessarily of the form $q_l(v)u^l\alpha^j$. A special case is when $j = 0$ in which case $\varphi(u)$ is in $\mathbf{k}[u]$ and φ can be thought as an *automorphism* of $\mathbf{k}[u]$[2].

Since u is of degree p over $\mathbf{K}[v]$ and $u^p = v$, we can define $T : \Omega \to \Omega$ by $T(u) = \alpha u$. For getting all possible morphisms $\mathbf{k}[u] \to \Omega$, it is then enough to look at the automorphisms of $\mathbf{k}[u]$ and to compose with a power of T.

An automorphism $\varphi_i : \mathbf{k}[u] \to \mathbf{k}[u]$ is completely determined by i such that $\varphi_i(u) = q_i(v)u^i$. We have $\varphi_i \circ \varphi_j = \varphi_{ij}$ and so the group of such automorphisms can be identified with a subgroup of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of the nonzero elements mod. p. Let g be a primitive root modulo p and choose $k = g^l$ mod. p which generates this group. We write $l\nu = p-1$. The corresponding automorphism satisfies

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

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 in Ω are then exactly the elements

$$u\alpha^i,\ \theta(u)\alpha^i, \ldots, \theta^{\nu-1}(u)\alpha^i$$

and hence u is of degree $p\nu$ over $\mathbf{k}$. It follows that the minimal polynomial of u over $\mathbf{k}$ is of the form

$$(X^p - v)\ldots(X^p - \theta^{\nu-1}(v))$$

and hence the polynomial $(Y - v)\ldots(Y - \theta^{\nu-1}(v))$ is irreducible in $\mathbf{k}[Y]$. Hence v is of degree ν over $\mathbf{k}$ and furthermore, v is the root of a *cyclic polynomial* of degree ν over $\mathbf{k}$.

We obtain in this way one result of Galois which characterizes the group of automorphisms of $\Omega = \mathbf{K}[u] = \mathbf{K}[x_0, \ldots, x_{p-1}]$ as a subgroup of the affine maps of $\mathbb{Z}/p\mathbb{Z}$. But Abel and Kronecker's analysis goes further and give a complete characterization of the form of the roots of a solvable polymomial.

2.2 Galois group

There are several Galois group involved. First $\mathbf{K}[u]$ is a normal extension of $\mathbf{K}$ and the Galois group is of order $p\nu$. The extension $\mathbf{k}[u]$ is in general not a normal extension of $\mathbf{k}$ (if $\mathbf{k}$ does not contain a primitive pth root of unity). However the extension $\mathbf{k}[v]$ is a normal extension of $\mathbf{k}$ with a cyclic group of order ν. There is also the extension $\mathbf{k}[x_0, \ldots, x_{p-1}]$ of $\mathbf{k}$, whose Galois group is of order $p\nu$[3]. Finally $\mathbf{K}[u] = \mathbf{k}[\alpha, u]$ is also a normal extension of $\mathbf{k}$ and its Galois group is analysed in the work [7].

2.3 A refinement and a complete characterisation

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

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

[2]This is equivalent to $\varphi(x_0) = x_0$, in which case φ permutes the elements of the sum

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

[3]It follows that P has the same Galois group over the fields $\mathbf{k}$ and $\mathbf{K}$. In general however the Galois group of P may change if we add to $\mathbf{k}$ roots of unity. This means that we cannot assume, like in the works [3, 10, 5], that the base fields contain all roots of unity.

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

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

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

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

with $r=h_0^t$. The elements $r=r_0,\ r_1,\ \dots,\ r_{\nu-1}$ have to be pairwise distinct since v is not of pth power in $\mathbf{K}[v]$[4]. It follows[5] 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

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

We have

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

3 Summary of the analysis

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

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

We assume that the element s is not a pth power in $\mathbf{k}[r]$ and we introduce $w^p=s$ with w 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

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

and we have

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

The elements $w,\ w_1,\ \dots,\ w_{\nu-1}$ are linearly independent over $\mathbf{k}[\alpha,r]$ since s is not a pth power in $\mathbf{k}[r]$, and hence also in $\mathbf{k}[\alpha,r]$ using Lemma 5.1, by hypothesis. It follows from this that the elements $s,\ s_1,\ \dots,\ s_{\nu-1}$ are pairwise distinct: if $s=s_1$ for instance we have w of the form $\alpha^k w_1$ which is impossible. Hence s is of degree ν over $\mathbf{k}$.

The element

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

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.

We can deduce directly from this form of the roots the main results of [7]. In particular notice that if we build in this way two elements x and y of degree p over $\mathbf{k}$ then these two elements are fixed by exactly the same automorphisms of Ω/k, namely the automorphisms that satisfy $\varphi(w_1)=w_{1+l}$ for some fixed l (and then $\varphi(w_i)=w_{i+l}$ for all i). It follows that we have $\mathbf{k}[x]=\mathbf{k}[y]$.

[4] This fact is best understood in the examples below. For instance for $p=5$ and we have $\nu=4$ and we consider $r_3^8r_2^4r_1^2r_0$, if we have $r_0=r_1=r_2=r_3$ then this becomes r_0^{15} and if $r_0=r_2$ and $r_1=r_3$ this becomes $r_0^5r_1^{10}$.

[5] This is a consequence of Abel's analysis of cyclic equations. Any element t in $\mathbf{k}[v]$ having ν distinct conjugates is such that $\mathbf{k}[t]=\mathbf{k}[v]$. 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 $\mathbf{k}$.

4 Example: solvable equations of degree 5

4.1 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 $u^5 = v$.

4.2 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 $\mathbf{k}[r]$. $\mathbf{k}[r] = \mathbf{k}[r_1]$ has an automorphism θ such that $\theta(r) = r_1$ and $\theta(r_1) = r$. Then if we consider the radical extension $w^5 = r^4 r_1$ of $\mathbf{k}[r]$ and $w_1 = w^4/r^3$, so that $w_1^5 = r_1^4 r = \theta(w^5)$. For any polynomials ψ_0 and ψ_1 such that $\psi_0(r) \neq 0$ or $\psi_1(r) \neq 0$ 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 exactly 5 conjugates in $\mathbf{k}[\alpha, w]$ with $\alpha^5 = 1$. Indeed 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

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

If w is sent to $\alpha^i w_1$ then r is sent to r_1 and x_0 is sent to

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

We see in this way that the conjugates of x_0 over $\mathbf{k}$ are exactly x_0, x_1, x_2, x_3, x_4.

4.3 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 have an automorphism θ of $\mathbf{k}[r]$ with $\theta(r_i) = r_{i+1}$. We consider the radical extension $w^5 = r^8 r_1^4 r_2^2 r_3$ and

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

and $w_{i+5} = w_i$ so that $\theta(w_i^5) = w_{i+1}^5$. 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 $\mathbf{k}$. Indeed w has 20 conjugates of the form $\alpha^l w_i$. if w is sent to one w_i then x_0 is not changed, and if w is changed to $\alpha^{ki} w_i$ then x_0 is sent to x_k.

There is in the reference [12] 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 $\nu = 4$. (It seems to be an open problem to know if the formula given by Abel in his letter to Crelle covers actually all possible cases or not.) 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 restriction is reproduced in [12]. On the other hand, Abel's work [3] considers all possible cases.

5 Abel's Analysis

The rest of the paper consists in a proof of Theorem 2.1, following closely Abel [3].

Notice first that if P is solvable in $\mathbf{k}$ it is solvable in any extension $\mathbf{L}$ of $\mathbf{k}$. Indeed given the sequence of radical extensions $\mathbf{k}_1,\ \ldots,\ \mathbf{k}_n$ of $\mathbf{k}$ it is direct to build a corresponding sequence $\mathbf{L}_1,\ \ldots,\ \mathbf{L}_n$ with a morphism $\mathbf{k}_i \to \mathbf{L}_i$ and where $\mathbf{L}_{i+1} = \mathbf{L}_i$ or $\mathbf{L}_{i+1}$ a radical extension of $\mathbf{L}_i$. If P has a root in $\mathbf{k}_n$ it has then a root in $\mathbf{L}_n$.

We assume that P is an irreducible solvable polynomial of degree p over $\mathbf{k}$. We show first that this implies that P is also irreducible over $\mathbf{K} = \mathbf{k}[\alpha]$.

Lemma 5.1 *P is irreducible over $\mathbf{K}$.*

Proof. Let $\alpha_1, \ldots, \alpha_l$ be the conjugates of α over $\mathbf{k}$. We have $l < p$. Let $Q(X, \alpha)$ be an irreducible factor of P in $\mathbf{K}[X]$. Then each $Q(X, \alpha_i)$ divides P. Since any root of $R(X) = Q(X, \alpha_1) \ldots Q(X, \alpha_l)$ is a root of P and P is irreducible, R is a power P^m of P. If d is the degree of Q this implies $pm = dl$, and since p is prime and $l < p$, we have $p = d$. □

If we assume that P is solvable over $\mathbf{k}$ it is also solvable over $\mathbf{K}$ and we have a sequence, that we can assume minimal, of radical extensions $\mathbf{K}_1 = \mathbf{K}[u_1]$, $\mathbf{K}_2 = \mathbf{K}[u_1, u_2], \ldots, \mathbf{K}_n = \mathbf{K}[u_1, \ldots, u_n]$ where $\mathbf{K}_n$ contains a root x_0 of the polynomial P and we have $u_i^{p_i}$ in $\mathbf{K}_{i-1}$ for some prime p_i and the equation $X^{p_i} = u_i^{p_i}$ has no solution, and hence is irreducible over $\mathbf{K}_{i-1}$. We write $u = u_n$. We can write

$$x_0 = q_0 + q_1 u + \ldots + q_{p_n - 1} u^{p_n - 1}$$

with $q_0, \ldots, q_{p_n - 1}$ in $\mathbf{K}_{n-1}$. A simple argument[6], which is already in [1], shows that we can assume $q_1 = 1$.

The element x_0 is of degree p_n over $\mathbf{K}_{n-1}$. Hence its degree over $\mathbf{K}$ is divisible by p_n. On the other hand, this degree is p since P is irreducible. Since p is prime we have $p = p_n$ and we see that $\mathbf{K}_n$ contains *all* the roots of P that are the conjugates of x_0

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

for $l = 0, \ldots, p-1$.

We have then

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

The element u is in $\mathbf{K}[x_0, \ldots, x_{p-1}]$. It is called that (Lagrange) *resolvent* of the equation $P(x) = 0$. 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 $\mathbf{K}[u]$, so that $\mathbf{K}[u] = \mathbf{K}[x_0, \ldots, x_{p-1}]$ and x_0 is in $\mathbf{k}[u]$. This will be a consequence of the fact that u is distinct from all elements

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

where $\sigma \in \mathfrak{S}_p$ is a non trivial permutation of $0, \ldots, p-1$.

The polynomial

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

is in $\mathbf{k}[X]$, since it is symmetric in the x_i and invariant by the change of α to α^j, and such that $Q(u) = 0$. If $R = Q/(X - u)$ we have R in $\mathbf{k}[u][X]$. We claim that $R(u) \neq 0$.

Lemma 5.2 *If $u_\sigma = u$ then $\sigma(l) = l$ for all l.*

Proof. (Abel) 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. □

[6] Since the sequence is minimal, at least one q_l, $l > 0$ is $\neq 0$. We have then $\mathbf{K}_{n-1}[q_l u^l] = \mathbf{K}_{n-1}[u]$ and if we replace u by $q_l u^l$ we see that x_0 gets the required form.

The element

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

is in $\mathbf{K}$, since it is symmetric in $x_0, \ldots, x_{p-1}$. Furthermore, the element $R(u)x_0$ is in $\mathbf{k}$, since it is also invariant when we change α to α^i.

We get in this way a proof of Theorem 2.1.

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] H. Edwards. Kronecker's Lost Theorem. Manuspcript, 2011.

[8] L. Kronecker, Über die algebraisch auflösbaren Gleichungen. Monatsber. Berlin, 1853, 365-374. *Werke*, vol. 4, 3-11.

[9] Malmstem. In solutionem aequationum algebraicorum disquisitio. Crelle 34 (1847), 30-45.

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

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

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