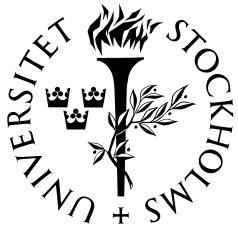

SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

The theory of Galois

av

Alexis Seferlis

2011 - No 1

The theory of Galois

Alexis Seferlis

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Torsten Ekedahl

2011

Abstract

Mathematicians of the 18th century had available methods to express the roots of polynomial equations of degree up to four in terms of the coefficients of the equation, but no method that would solve an arbitary quintic or higher degree equation. Lagrange observed that all these methods are ruled by a single pattern based on symmetry. Later on Évariste Galois realized that the appearance of symmetry was a consequence of properties of an asymmetry, namely a function/expression of the roots of the equation, nowadays called the Galois resolvent, which is not symmetric at all and is such that the roots can be rationally expressed in terms of this function. The Galois resolvent when interpreted as an element of a certain field gives rise to a group, nowadays called the Galois group, which will be characterized as the group consisting of those permutations of the roots of the polynomial that leave rational expressions in the roots, which lie in the field, unaltered. The property of a polynomial being solvable over a field will be described in terms of its Galois group. Finally, we present the modern formulation of Galois Theory of finite field extensions due to Emil Artin.

Contents

1 Introduction

1.1 Field extensions

In this section we recall some basic facts from a first course in abstract algebra.

$\circ$

Let F be a field. A subfield of F is a subset of F which is itself a field under the operations of F, an extension E of F is a field which has F among its subfields. The term field extension refers to a pair of fields (E, F) where $F \subset E$ and is denoted by E/F, also F is called the base field of the field extension E/F. An intermediate field of a field extension E/F is a field L that contains F, but is contained in E. A field isomorphism is a ring isomorphism between two fields.

Definition 1.1.1 Let E be an extension of a field F and Y a subset of E. The intersection of all intermediate fields of the extension E/F that contains both F and Y is a field. It is called the extension field of F obtained by adjoining Y and is denoted by $F(Y)$. When $Y = \{a_1, ..., a_n\}$ we simply write $F(a_1, ..., a_n)$ and if Y contains just one element then $F(Y)$ is called a simple field extension of F.

Proposition 1.1.1 Let E be a field extension of F and α an element in E. Then, $F(\alpha) = \{f(\alpha)/g(\alpha) : f, g \in F[x], g(\alpha) \neq 0\}$.

Proof: An element that can be rationally expressed in terms of a and elements in F belongs to every intermediate field of the extension E/F that contains both F and α, hence it belongs to their intersection $F(\alpha)$. Conversely, consider the map $\phi : F[x] \to E$ given by $f(x) \mapsto f(\alpha)$. This map is clearly a ring homorphism. Hence the set $\{f(\alpha) : f \in F[x]\}$ being the image of the ring homorphism ϕ is itself a ring. But, $\{f(\alpha)/g(\alpha) : f, g \in F[x], g(\alpha) \neq 0\}$ is the quotient field of the integral domain $\{f(\alpha) : f \in F[x]\}$ and as it contains both F and α the other inclusion follows.

Definition 1.1.2 Let E be an extension field of F and α an element in E. If there exists a nontrivial polynomial p over F such that $p(\alpha) = 0$, then α is an algebraic element over F. A field extension E/F is called algebraic if every element in E is algebraic over F.

Let E/F be a field extension, α a an element in E and $\phi : F[x] \to E$ the ring homorphism given by $f(x) \mapsto f(\alpha)$. The image of ϕ which is $\{f(\alpha) : f \in F[x]\}$ is isomorphic to $F[x]/ker(\phi)$. The kernel of ϕ is simply $ker(\phi) = \{f(\alpha) = 0 : f \in F[x]\}$ hence when α is algebraic over F the kernel

is not the zero-set. Now, as F is a field it follows that $F[x]$ is a principal ideal domain hence $\mathrm{k}er(\phi) = (q)$ for some polynomial $q \in F[x]$. Observe that in (q) there is a family of polynomials of the same degree k such that there is no polynomial in (q) of degree smaller than k. We give emphasis to the monic polynomial which lies in the family.

Definition 1.1.3 The minimal polynomial of an algebraic element α over F is the monic polynomial of least degree over F that has α as a root and we denote it by m_α.

By definition, $m_\alpha(\alpha) = 0$ hence q divides m_α. It follows again by definition that m_α divides q . Hence, $\mathrm{k}er(\phi) = (m_\alpha)$.

Proposition 1.1.2 Let E/F be a field extension and $\alpha \in E$ an algebraic element over F

(1) The minimal polynomial of α over F is irreducible. A polynomial p in $F[x]$ has α as a root iff $m_\alpha \mid p$.

(2) Let n be the degree of m_α, then $F(\alpha) = \{a_0+a_1\alpha+...+a_n\alpha^{n-1} : a_i \in F\}$.

Proof: (1) If it is not irreducible, then there exists an irreducible factor q of m_α of less degree than m_α and with α as a root, contradiction. Next, by the above arguments it follows that p is a polynomial over F with α as a root if and only if p lies in the ideal generated by (m_α).

(2) Every element that can be polynomially expressed in terms of α and elements in F is an element in $F(a)$. Conversely, let $\phi : F[x] \to E$ be the ring homorphism given by $f(x) \mapsto f(\alpha)$. Clearly, the image of ϕ consists of elements $a_0+a_1\alpha+...+a_k\alpha^k : \ k \in \mathbb{N},\ a_i \in F$. But as $\alpha^n = b_0+b_1\alpha+...+b_n\alpha^{n-1}$ for some $b_i \in F$ it follows by induction that every power of α can be expressed as a linear combination of the elements $1, \alpha, ..., \alpha^{n-1}$ over F and so that $\mathrm{i}m(\phi) = \{a_0 + a_1\alpha + ... + a_n\alpha^{n-1} : a_i \in F\}$. Now, $\mathrm{i}m(\phi)$ is a field since it is isomorphic to the ring $F[x]/(m_\alpha)$ which is a field as m_α is irreducible. The rest follows from the definition of $F(a)$.

Given a field extension E/F, then E can be considered as a vector space over F in a natural way by interpreting F as an additive group and by defining scalar multiplication as multiplication in E. The dimension of E as a vector space over F is called the degree of the extension E/F, and is denoted by $[E : F]$. If $[E : F] < \infty$ then E is called a finite extension of F.

Corollary 1.1.1 Let α be an algebraic element over a field F. If $deg(m_\alpha) = n$ then a basis of $F(a)$ over F is given by $\{1, \alpha, ..., \alpha^{n-1}\}$ and therefore $[F(\alpha) : F] = n$

Proof: By Proposition 1.1.2 (2) it follows that the elements $1, \alpha, ..., \alpha^{n-1}$ span $F(a)$. Suppose that they are not linearly independent, then there exist elements $b_0, b_1, ..., b_{n-1} \in F$ not all zero such that $b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = 0$. But, then m_α is not the polynomial of least degree over F with α as a root, contradiction.

Proposition 1.1.3 If E/F is a finite field extension, say $[E : F] = n$, then E is algebraic over F.

Proof: Let a be an element in E. The elements $1, a, ..., a^n$ are linearly dependent over F, hence there exists $b_0, b_1, ..., b_n \in F$ not all zero such that $b_0 + b_1a + ... + b_na^n = 0$.

Theorem 1.1.1 If $F \subset L \subset E$ are three fields then $[E : F] = [E : L][L : F]$.

Proof: For simplicity assume that E is a finite extension of L and L a finite extension of F. Let $\{a_i\}_{i=1}^n$ be a basis for E over L and $\{b_j\}_{j=1}^m$ a basis for L over F, then $\{a_ib_j\}$ span E. To see this let x be an element in E then,
$x = \sum_{i=1}^{m} l_ia_i$ for some $l_i \in L$ and $l_i = \sum_{i=1}^{m} f_{ij}b_j$ for some $f_{ij} \in L$ so
$x = \sum_{i=1}^{m} (\sum_{j=1}^{m} f_{ij}b_j)a_i = \sum_{i=1}^{m}\sum_{j=1}^{m} f_{ij}a_ib_j.$
Also, $\{a_ib_j\}$ are linearly independent over F since if $f_{ij} \in F$ are such that

$\sum_{i=1}^{m}\sum_{j=1}^{m} f_{ij}a_ib_j = 0$ then $\sum_{i=1}^{m} (\sum_{j=1}^{m} f_{ij}b_j)a_i = 0$ as the a_i's are linearly

independent over L we get $\sum_{j=1}^{m} f_{ij}b_j = 0$ and as the b_j's are linearly

independent over F we finally get $f_{ij} = 0$ for all i, j.

Proposition 1.1.4 Let E be an extension field of F and $\alpha_1, ..., \alpha_n$ elements of E that are algebraic over F. Then, $[F(\alpha_1, ..., \alpha_n) : F] < \infty$.

Proof: We use induction on the number of elements adjoined to an intermediate field of the extension E/F. Let L be an intermediate field and α an element algebraic over L, then $[L(a) : L] < \infty$ by Corollary 1.1.1. Assume that the proposition holds true whenever less than n algebraic elements are

adjoined to F. Let, now, $\alpha_1, ..., \alpha_n$ be algebraic elements over F. By Theorem 1.1.1 it follows that
$[F(\alpha_1, ..., \alpha_n) : F] = [F(\alpha_1, ..., \alpha_n) : F(\alpha_1, ..., \alpha_{n-1})][F(\alpha_1, ..., \alpha_{n-1}) : F]$.
By the induction hypothesis, $[F(\alpha_1, ..., \alpha_n) : F(\alpha_1, ..., \alpha_{n-1})] < \infty$ and $[F(\alpha_1, ..., \alpha_{n-1}) : F] < \infty$. Hence, the result follows.

Given a polynomial over a field F, the following very important theorem allows one to speak about the roots of the polynomial since it follows from it that they will exist in a finite algebraic extension of F.

Notation: Let $i : F \to F'$ be a field isomorphism, if $p = c_0 + ... + c_n x^n$ is a polynomial over F denote by $i(p)$ the polynomial $i(c_0) + ... + i(c_n)x^n$ over F'.

Theorem 1.1.2 A polynomial p over a field F has a root in an extension field E of F.

Proof: We can assume without loss of generality that $p = a_0 + a_1 x + ... + a_n x^n$ is irreducible, since otherwise pick an irreducible factor of p. As p is an irreducible polynomial over F the principal ideal generated by p in $F[x]$ is maximal hence $F[x]/(p)$ is a field. The map $i : F \to F[x]/(p)$ given by $f \mapsto f + (p)$ is an injective ring homorphism hence F is a field that is isomorphic to the subfield $i(F) = \{f + (p) : f \in F\}$ of $E = F[x]/(p)$. If we identify F with $i(F)$ then F can be considered as a subfield of E and so E as an extension field of F. Then $x + (p)$ is a root of p in E, since

$$\begin{aligned} p\big(x + (p)\big) &= a_0 + a_1\big(x + (p)\big) + ... + a_n\big(x + (p)\big)^n \\ &= \big(a_0 + (p)\big) + \big(a_1 x + (p)\big) + ... + \big(a_n x^n + (p)\big) \\ &= a_0 + a_1 x + ... + a_n x^n + (p) = 0. \end{aligned}$$

1.2 Solvable equations

From now on and until the end of chapter 3 we let the symbol F stand for an arbitary field of characteristic zero.

$\circ$

With an understanding of the *essence* of the notion of a field extension we are able to go further than what seems apparently to be a satisfactory definition of solvability: 'A polynomial p over a field F is called solvable if we can arrive at concrete formulas that express the roots of p in terms of elements in F by making use, a finite number of times, of the operations addition, substraction, multiplication, division and extraction of roots'. Hence,

according to this definition we require the roots to lie in a finite field extension of F. But, instead of trying to find explicit formulas for the roots in terms of elements in F it turns out be very fruitful to try to describe in the simplest manner as possible an 'eligible' field extension of F(where the roots exist). For this purpose, let us, as a first step, try to solve the cubic equation over $\mathbb{Q}$ according to Cardano and try to interpret our result in terms of fields. After dividing all the coefficients of the cubic with its leading coefficient we obtain

$$x^3 + ax^2 + bx + c = 0 \quad \text{where} \quad a, b, c \text{ belong to } \mathbb{Q} \tag{2.1}$$

Making a change of variables $y = x + \frac{a}{3}$ in order to eliminate the quadratic term we get

$$y^3 + py + q = 0 \quad \text{where } p = \frac{3b - a^2}{3} \text{ and } q = \frac{27c - 9ab + 2a^3}{27} \tag{2.2}$$

Set $y = u + v$, then

$$u^3 + v^3 + (3uv + p)uv + q = 0 \tag{2.3}$$

Imposing the condition $3uv + p = 0$ and using it in (2.3) we see that u, v satify the sextic equation

$$w^6 + qw^3 - \frac{p^3}{27} = 0 \tag{2.4}$$

The above equation is a quadratic for w^3 and hence it can be solved, therefore u^3 and v^3 are determinable quantities and so are u and v. Hence, a possible solution for equation (2.2) can be represented in the form

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \tag{2.5}$$

A straightforward verification shows that there is a root corresponding to the formula (2.5) and hence by taking in consideration the restriction imposed we can verify that the other two roots of equation (2.2) are given by

$$x = \omega \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \tag{2.5}$$

$$x = \omega^2 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \tag{2.5}.$$

Now, we have to trace back the operations that lead us to the final form of the roots. We single out the operation of extracting roots and this simply because if we have algebraic relations over some field F and involving unknowns then by a root extraction of an element in F, in those relations, we 'transfer' the relations to the simple field extension obtained by adjoining the extracted element to F. Taking a sequence of root extractions we create a sequence of simple field extensions:

$$\sqrt{\frac{p^3}{27}+\frac{q^2}{4}} \quad \rightsquigarrow \quad \mathbb{Q}(\sqrt{\frac{p^3}{27}+\frac{q^2}{4}})/\mathbb{Q}, \qquad a_1 = \sqrt{\frac{p^3}{27}+\frac{q^2}{4}}, \;\; F_1 = \mathbb{Q}(a_1)$$

$$\sqrt[3]{-\frac{q}{2}+a_1} \quad \rightsquigarrow \quad F_1(\sqrt[3]{-\frac{q}{2}+a_1})/F_1, \;\; a_2 = \sqrt[3]{-\frac{q}{2}+a_1}, \;\; F_2 = F_1(a_2)$$

$$\sqrt[3]{-\frac{q}{2}-a_1} \quad \rightsquigarrow \quad F_2(\sqrt[3]{-\frac{q}{2}-a_1})/F_2, \;\; a_3 = \sqrt[3]{-\frac{q}{2}-a_1}, \;\; F_3 = F_2(a_3)$$

$$\omega(=\sqrt[3]{1}) \quad \rightsquigarrow \quad F_3(\omega)/F_3$$

This illustration partially motivates the following two definitions (they can be found non-formalized among the pages of Galois' manuscript: *Mémoire sur les conditiones de résolubilité des équations par radicaux*)

Definition 1.2.1 Let F be a field a radical extension E of F is a field extension E/F for which there exist intermediate fields $F_1, ..., F_n$ such that :
(1) $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{n-1} \subseteq E = F_n$,
(2) $F_{i+1} = F_i(a_i)$ where $a_i^{p_i} \in F$ for some prime p_i (or p_i=1).

Definition 1.2.2 A polynomial p over F is called solvable if its roots lie in a radical extension of F.

According to Definition 1.2.2 we can directly see that the binomial equations over any field, i.e $x^n - a$ where n is an integer, are solvable. The class of polynomials for which $a = 1$ have some very interesting properties. For example, if we have a root α of a binomial equation $p(x) = x^m - a = 0$ then we get the other roots of p simply by multiplying α with the roots of the equation $x^m - 1 = 0$. Shortly, we will see other properties but let us first give a definition:

Definition 1.2.3 Let F be a field. The roots of the equation $x^n - 1 = 0$ are called the n-th roots of unity of F.

It is a well-known fact that the n-th roots of unity of $\mathbb{Q}$ are given by the formula (and that these n numbers are distinct)

$$e^{\frac{2\pi ik}{n}} = \cos(\tfrac{2\pi ik}{n}) + i\sin(\tfrac{2\pi ik}{n}), \quad \text{where } k = 1, 2, ..., n. \tag{2.6}$$

For small values of n we can without much effort get simple expressions for the n-th roots of unity in terms of radicals that are given by binomial equations of smaller degree than n. For example, the nontrivial third roots of unity satisfy the equation $\frac{x^3-1}{x-1} = x^2 + x + 1 = 0$. This is a quadratic with roots $\frac{1+\sqrt{-3}}{2}$ and $\frac{1-\sqrt{-3}}{2}$. The 5-th roots of unity, except 1, satisfy the quartic equation

$$x^4 + x^3 + x^2 + x + 1 = 0.$$

If we do not want to use the formula of Ferrari(see [9]) for the quartic we can divide equation (2.7) by x^2 and then make a change of variables $y = x + 1/x$ to get the following equation for y:

$$y^2 + y - 1 = 0.$$

Hence, $y = \frac{-1 \pm \sqrt{5}}{2}$ and the wanted four values of x can be found by solving the two equations $x^2 - \frac{-1 \pm \sqrt{5}}{2}x + 1 = 0$. So,

$$x = \frac{\sqrt{5} - 1 \ \pm \sqrt{-10 \ - 2\sqrt{5}}}{4}, \qquad x = \frac{\sqrt{5} - 1 \ \pm \sqrt{-10 \ + 2\sqrt{5}}}{4}.$$

In the same manner we can find the 7-th roots of unity. Namely, divide $x^6 + ... + x + 1$ with x^3 then set $y = x + x^{-1}$ and express the sums $x^n + x^{-n}$, $n = 1, 2, 3$ in terms of this new variable to get an equation of degree three in y. Finally, the relation $x^2 - xy + 1 = 0$ can give us the 7-th roots of unity(except 1). But, this method will not be successful by itself if we try to solve the equation which yields the 11-th roots of unity:

$$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0. \tag{2.7}$$

The reason for this is that the equation we will obtain will be a quintic in y and we do not have a formula which solves an arbitary quintic. A solution for the above quintic, that is, the explicit expression of the roots in terms of roots of binomial equations of degree equal or less than five was first given by Vandermonde. A very nice presentation of his solution accompanied by comments can be found in [8]. The fact that interest us and which can be shown by a straightforward generalization of the arguments of Vandermonde is that an arbitary n-th root of unity of a field F lie in a pure

radical extension of F:

Definition 1.2.4 Let F be a field. A pure radical extenion, briefly pr-extension, E of F is a field extension E/F for which it exists a chain of fields $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{n-1} \subseteq E = F_n$ with the following properties
(1) $F_{i+1} = F_i(a_i)$ where ${a_i}^{p_i} \in F$ for some prime p_i (or $p_i = 1$),
(2) The polynomial $x^{p_i} - {a_i}^{p_i}$ is irreducible over F_i and
(3) F_i contains a primitive p_i-th root of unity for $i = 1, ..., n-1$.

The set of all n-th roots of unity $\mathbb{Q}$ under multiplication form a group, call this group $\mathbb{P}_n$. Looking back at formula (2.6) we see that the n-th root of unity given by $\rho = \cos(\frac{2\pi i}{n}) + i\sin(\frac{2\pi i}{n})$ has the property that all the the other n-th roots of unity are powers of ρ, that is, ρ generate $\mathbb{P}_n$. The other generators of $\mathbb{P}_n$ are, clearly, $e^{\frac{2\pi ik}{n}}$ where k is relatively prime to n. The generators of $\mathbb{P}_n$ are called the primitive n-th roots of unity and we denote by $\tilde{\mathbb{P}}_n$ the set of all primitive n-th roots of unity. Primitive n-th roots of unity are similarly defined for any field F.

Definition 1.2.5 The polynomial Φ_n, for any $n \in \mathbb{N}$, over $\mathbb{C}$ defined by

$$\Phi_n(x) = \prod_{\zeta}(x - \zeta),$$

where ζ varies over the set of primitive n-th roots of unity is called the n-th cyclotomic polynomial.

Proposition 1.2.1 The n-th cyclotomic polynomial is a polynomial over $\mathbb{Z}$.

Proof: We argue inductively, for the 1-th cyclotomic the proposition is true. Assume that all k-th cyclotomic polynomials where k is smaller than n have integral coefficients. Now, let us call the number d the order of an n-th root of unity ω if it is the smallest positive integer such that $\omega^d = 1$. Let ω_0 be a root of unity of order d then all the d-th roots of unity are given by $\omega_0^i,\ i = 1, .., d$ hence ω_0 is a primitive d-th root of unity. Therefore, we can partition the set of all n-th roots of unity as follows $\mathbb{P}_n = \{\zeta : \zeta^n - 1 = 0\} = \bigcup_{d|n}\{\zeta : \zeta^d - 1 = 0 \text{ and } \zeta \text{ has order } d\} = \bigcup_{d|n}\tilde{\mathbb{P}}_d$ and so we get the identity $x^n - 1 = \prod_{d|n}\Phi_d$. Set $p = \prod_{d|n,\ d\neq n}\Phi_d$ then, by induction, p is a polynomial in $\mathbb{Z}$. Finally, with p as a factor of $x^n - 1$ it follows from the Euclidean division algorithm for polynomials over $\mathbb{Q}$ that Φ_n is a polynomial with rational coefficients. But, p is monic and so Φ_n has integral coefficients.

The following two facts will be used chapter 2.

Lemma 1.2.1 For prime p, the polynomial $x^p - a$ is irreducible over F if and only if a is not a p-th power of an element in F.

Proof: Assume that a is not a p-th power of an element in F. Then a^i is not either a p-th power of an element in F for $i = 2, \ ... \ , \ n-1$. To see this, suppose that b is an element in F such that $b^p = a^i$. Since i and p are relatively prime there exist integers c, d such that $ic + pd = 1$. Hence, a is the p-th power of the element $b^c a^d$, contradiction. Now, let α be an element in an extension field of F such that $\alpha^p = a$. It suffices to show that the polynomial $\prod_{\zeta \in Y} (x - \zeta\alpha)$, where Y is a proper subset of the set containing all the p-th roots of unity, is not a polynomial over F. If it were, then $\prod_{\zeta \in Y} \zeta\alpha$ should be an element in F which in turns implies,

$$\big(\prod_{\zeta \in Y} \zeta\alpha\big)^p = \big(\prod_{\zeta \in Y} \zeta \times \alpha^{|Y|}\big)^p = \big(\alpha^{|Y|}\big)^p = \big(\alpha^p\big)^{|Y|} = a^{|Y|},$$

that $a^{|Y|}$ is a p-th power of an element in F, contradiction. The converse is clear.

Proposition 1.2.2 Let E be an extension field of F for which there exist elements $a_1, ..., a_n \in E$ such that $E = F(a_1, ..., a_n)$ and $a_i^n \in F$ for some integer n. If F contains a primitive n-th root of unity then E is a pure radical extension of F.

Proof: Firslty, make the additional assumption that E is a simple field extension of F, that is $E = F(a)$ for some $a \in E$. If $a \in F$, then E is a pure radical extension of F. Assume that the proposition is true for all simple field extensions for which the exponent of a is smaller that n. Now, let E be a field extension of F such that $E = F(a)$ and $a^n \in F$. Suppose that n is prime, then either a^n is an n-th power of an element in F or it is not. If it is then $\alpha^n = a^n$ for some $\alpha \in F$ and so $\alpha = a\zeta^m$ where ζ is a primitive n-th root of unity and m some integer, hence $\alpha \in F$. If it isn't, then $x^n - a^n$ is irreducible over F by Lemma 1.2.1. Suppose that n is composite, then $n = n_1 n_2$ for some nonunit integers. As $(a^{n_1})^{n_2} \in F$ it follows by induction that $F(a^{n_1})$ is a pure radical extension of F and as $a^{n_1} \in F(a^{n_1})$ it follows, by induction, that $F(a)$ is a pure radical extension $F(a^{n_1})$, hence $F(a)$ is a pure radical extension of F. The "general" case follows by considering the chain $F \subset F(a_1) \subset F(a_1, a_2) \subset ... \subset F(a_1, ..., a_n)$.

2 Historical recursion

2.1 Réflexions sur la résolution algébrique des équations

The group of all permutations of n arbitary letters will be identified with the symmetric group S_n. Additionaly, in this section we have to think of the roots $x_1, ..., x_n$ of a polynomial p as indeterminates instead of them having fixed values and so a field on which p can be defined must contain the elementary symmetric polynomials $\sigma_1, ..., \sigma_n$ in the variables $x_1, ..., x_n$ (see Apppendix).

$\circ$

The importance of permutations in the study of equations became clear after Lagranges' publication. By introducing symbols for the permutations of n elements and by studying the effect that permutations of the roots had on rational functions of the roots he was able to make fruitful observations and to prove important theorems. Lagrange's theorem is known to all mathematicians and states that the order of a group is divisible by the order of any of its subgroups is among them.

Concerning the solvability of the general equation which was the core of his investigations, he put the known techniques for solving polynomials of degree up to four in a common frame. More precisely, indepedentely of the chosen method the solution of an equation depended on other auxiliary equations called réduites. The roots of the auxiliary equations were rational functions of the roots to be found $x_1, ..., x_n$ and conversely the roots to be found could be rationally expressed in terms of the roots of the auxiliary equations. Since the former could be given expressions by radicals so could the latter. This is Lagranges' own words :

"On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution des équations, que ces méthodes se réduisent toutes à un même principle général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles: (1) que l'équation ou les équations par lesquelles elles seront données, c'est-á-dire dont elles seront les racines(équations qu'on nomme communément les réduites), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations d'un degré moindre que celui-lá; (2) que l'on puisse en déduire aisément les valeurs des racines cherchées.[1]

Example 2.1.1 Let us see how this pattern explains the solution of the general cubic, whose coefficients are considered as intermediates. After dividing all the coefficients of the cubic with its leading coefficient we obtain

[1] An english translation can be found in [5].

$x^3 + ax^2 + bx + c = 0$. By setting $y = x + a/3$ the equation reduces to $y^3 + py + q = 0$, where $p = \frac{3b-a^2}{3}$ and $q = \frac{27c-9ab+2a^3}{27}$, since the roots x_1, x_2, x_3 of the initial equation can be found from those of the reduced by substracting $a/3$. The roots of the reduced equation are

$$y_1 = \sqrt[3]{\frac{q}{2} + \sqrt{r}} + \sqrt[3]{\frac{q}{2} - \sqrt{r}}$$

$$y_2 = \zeta^2 \sqrt[3]{\frac{q}{2} + \sqrt{r}} + \zeta \sqrt[3]{\frac{q}{2} - \sqrt{r}}$$

$$y_3 = \zeta \sqrt[3]{\frac{q}{2} + \sqrt{r}} + \zeta^2 \sqrt[3]{\frac{q}{2} - \sqrt{r}},$$

where $r = q^2/4 + p^3/27$ and ζ is a primitive third root of unity, say $\zeta = (-1 + \sqrt{-3})/2$.

The auxiliary equations used to construct the above expressions are

(1) $x^2 + qx - p^3/27 = 0$ with roots $x = q/2 \pm \sqrt{r}$,

(2) $x^3 = q/2 + \sqrt{r}$ with roots $z_1 = \sqrt[3]{\frac{q}{2} + \sqrt{r}}$, $z_2 = \zeta z_1$, $z_3 = \zeta^2 z_1$

(3) $x^3 = q/2 - \sqrt{r}$ with roots $z_4 = \sqrt[3]{\frac{q}{2} - \sqrt{r}}$, $z_5 = \zeta z_4$, $z_6 = \zeta z_4$.

The roots x_1, x_2, x_3 can be rationally expressed in terms of $z_1, ..., z_6$. But, the later roots can also be rationally expressed in terms of former as the following identities holds:

$$\sqrt[3]{\frac{q}{2} + \sqrt{r}} = 1/3(x_1 + \zeta x_2 + \zeta^2 x_3)$$

$$\sqrt[3]{\frac{q}{2} - \sqrt{r}} = 1/3(x_1 + \zeta^2 x_2 + \zeta x_3).$$

And so,

$$z_1 = 1/3(x_1 + \zeta x_2 + \zeta^2 x_3) \qquad z_4 = 1/3(x_1 + \zeta^2 x_2 + \zeta x_3)$$

$$z_2 = 1/3(\zeta x_1 + \zeta^2 x_2 + x_3) \qquad z_5 = 1/3(\zeta x_1 + x_2 + \zeta^2 x_3)$$

$$z_3 = 1/3(\zeta^2 x_1 + x_2 + \zeta x_3) \qquad z_6 = 1/3(\zeta^2 x_1 + \zeta x_2 + x_3)$$

We observe that the roots $z_1, ..., z_6$ of the auxiliary equations which are rational expressions in the roots x_1, x_2, x_3 can be obtained by taking one of these expressions, say z_1, and then by permuting the roots x_1, x_2, x_3 in the expression in all possible ways we get the other, that is, z_1 assumes 6 distinct values under the action of the symmetric group. Additionaly, z_1^3

assumes only two distinct values, under the action of the symmetric group, as $z_1^3 = z_2^3 = z_3^3$ and $z_4^3 = z_5^3 = z_6^3$. On the other hand, z_1 satisfies a sextic and z_1^3 satisfies a quadratic equation.

Proposition 2.1.1 Let f be a rational function in the variables $x_1, ..., x_n$ over the field $\mathbb{C}$. If f assumes m distinct values under the action of the symmetric group then f is a root of an irreducible polynomial Θ over $\mathbb{C}(\sigma_1, ..., \sigma_n)$ of degree m where $\sigma_1, ..., \sigma_n$ are the elementary symmetric polynomials in $x_1, ..., x_n$.

Scholium: This is relatively easy to prove. But it is more interesting to see this proposition in a broader context, the easiest way is to visit the website *http://gallica.bnf.fr* and search for volume 3 of Oeuvres de Lagrange pp. 205-421.

One can also find the following fact among the pages of Réflexions which in some sense generalizes the previous proposition.

Proposition 2.1.2 Let f and g be two rational functions in the variables $x_1, ..., x_n$ over $\mathbb{C}$. If f asummes m distinct values under the permutations that leave g invariant then f is a root of a polynomial of degree m with coefficients in $\mathbb{C}(g, \sigma_1, ..., \sigma_n)$.

Sholium: See volume 3 of Oeuvres de Lagrange pp. 205-421. Due to its importance this theorem is discussed in detail in the article of Kiernan ([5]) and with proof in the book of Tignol ([8]).

Let us write down the following functions of the roots,

$\phi_1 = x_1 + x_2 + x_3$

$\phi_2 = (1/3(x_1 + \zeta x_2 + \zeta^2 x_3))^3$

$\phi_3 = 1/3(x_1 + \zeta x_2 + \zeta^2 x_3))$

$\phi_4 = x_1$

If we think of the functions as elements in the rational function field of x_1, x_2, x_3 over $\mathbb{C}$ and as we consider every element in $\mathbb{C}(p, q)$ as known then Proposition 2.1.1 tells us that ϕ_2 can be found by solving a quadratic since it assumes only two distinct values under the permutations of the roots x_1, x_2, x_3. Also, ϕ_3 can be found from ϕ_2 by taking a cube root. Finally, the root x_1 can be found rationally from ϕ_3 by Proposition 2.1.2 since the only permutation of the roots x_1, x_2, x_3 that leave ϕ_3 invariant is the identity.

So, the solvability of the cubic which depended on the reduites can now be descibred in terms of the roots of the reduites which are of functions of the roots.

Preceeding to the solvability of the general equation of any degree the frame should be based on the same principles. Namely, the auxiliary equations must be either binomials of the same degree or equations of smaller degree where in both cases the coefficients of the equations can be algebraically determined. And hence on rational functions of the roots that are either n-th powers of other rational functions that can be expressed by radicals or assumes less than n distinct values under the permutations which leave other rational functions,which are expressible by radicals, invariant. All these statements can be given the following order:

Lagrange's criterion of solvability

The general polynomial f over $\mathbb{C}(\sigma_1, ..., \sigma_n)$ of degree n is solvable if one can find rational functions $\phi_1, ..., \phi_m$ over $\mathbb{C}$ in the roots $x_1, ..., x_n$ such that

ϕ_1 is a rational function symmetric in the roots $x_1, ..., x_n$ so by the fundamental theorem of symmetric polynomials it is expressible in terms of the coefficients of f, hence ϕ_1 is a known quantity.

ϕ_2 is either an n-th power of of ϕ_1 or assumes less than n distinct values under the action of the symmetric group,

ϕ_3 is either an n-th power of of ϕ_2 or assumes less than n distinct values under the permutations that leaves ϕ_2 invariant,

...

ϕ_k is either an n-th power of of ϕ_{k-1} or assumes less than n distinct values under the permutations that leaves ϕ_{k-1} invariant,

...

ϕ_{m-1} is either an n-th power of of ϕ_{m-2} or assumes less than n distinct values under the permutations that leaves ϕ_{m-2} invariant,

ϕ_m is one of the roots and is either ...

For equations that do not exceed the fourth degree, Lagrange stressed that, the simplest function, nowdays called Lagrange resolvent, that yield their solution can be represented by the general formula:

$$t_\omega = x_1 + \omega x_2 + \omega x_3 + ... + \omega^{n-1} x_n, \tag{2.1.1}$$

where $x_1, ..., x_n$ are the roots of the proposed equation of degree n and where ω is an n-th root of unity other than 1. This means two things, (1) the roots $x_1, ..., x_n$ can be rationally expressed in terms of the t_ω, (2) that t_ω is a root of a solvable equation. (1) which will be important in the following sections and which actually holds for any value of n follows by the formula [2],

$$x_{i+1} = \frac{1}{n}\Big((x_1 + ... + x_n) + \sum_\omega \omega^{-i} t_\omega\Big), \quad \text{for } i = 0, ..., n-1. \tag{2.1.2}$$

and by the fact that any t_ω can be rationally expressed in terms of any other $t_{\omega'}$ (follows by proposition 2.1.3). Both Vandermonde and Lagrange succeded in showing (2); we have demonstrated it for the cubic. For the quintic (2) does not hold since Lagrange (if I'm not mistaken and Vandermonde) showed that t_ω^5 is not a root of a polynomial of degree less than five whose coefficients can be algebraically determined. Hence, if a general formula for the quintic exists then it should depend on some functions of the roots other than (2.1.1). But, do such functions exist? No!, the first to study this question with succesion was Ruffini and the complete answer came from the mathematician Niels Henrik Abel.

2.2 The cyclotomic equation

If one studies the work of Vandermonde concerning the 11-th cyclotomic polynomial one will observe that:

"Not all permutations of the roots of the cyclotomic equation preserve the relations among the roots and it should be of importance to study those that the preseve them."

Unfortunately, we will not discuss the work of Vandermonde nor shall we discuss the decomposition, due to Gauss, of the cyclotomic equation to smaller degree equations since their work is of historical importance but out of the scope of this 'examensarbete'. The interested reader is refered to the article Mémoire sur la résolution des équations of Vandermonde, to Disquisitiones Arithmeticae of Gauss and to the book [8]. Now, our main aim in this section is to prove Theorem 2.2.3 which is obtained as a consequence of a generalization of the arguments of Vandermonde.

∘

[2] For a derivation of this formula look at pp. 135-136 of [8]

A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be primitive if the greatest common divisor of its coefficients is 1.

Lemma 2.2.1(Gauss' Lemma) The product of two primitive polynomials in $\mathbb{Z}[x]$ is a primitive polynomial.

Proof: Assume that f, g are two primitive polynomials then,

$f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, where $a_i \in \mathbb{Z}$ and $(a_0, ..., a_n) = 1$

$g = b_m x^m + b_{m-1}x^{m-1} + ... + b_0$, where $b_i \in \mathbb{Z}$ and $(b_0, ..., b_m) = 1$.

Let $p \in \mathbb{N}$ be a prime, and let i, j be the two indices that satisfy: $p \nmid a_i$ and $p \mid a_k$ for $0 \leq k \leq i-1$, $p \nmid b_j$ and $p \mid b_k$ for $0 \leq k \leq j-1$. Then, $fg = c_{n+m}x^{n+m} + ... + c_{i+j}x^{i+j} + ... + c_0$ and the coefficient c_{i+j} is not divisible by p. Since,

$c_{i+j} = \sum_{n=0}^{i-1} a_n b_{i+j-n} + a_i b_j + \sum_{n=0}^{j-1} a_{i+j-n} b_n$.

Clearly, the first and the third summand are divisible by p and the middle term is not.

Corrollary 2.2.1 Assume that a monic polynomial f in $\mathbb{Z}[x]$ is divisible by a monic polynomial g in $\mathbb{Q}[x]$. Then, $g \in \mathbb{Z}[x]$.

Proof: By assumption, $f = gh$ where $h \in \mathbb{Q}[x]$ and h monic. Hence,

$$g = x^n + \sum_{i=0}^{n-1} \frac{s_i}{t_i} x^i, \quad s_i, t_i \text{ are integers such that } (s_i, t_i) = 1$$

$$h = x^m + \sum_{i=0}^{m-1} \frac{s_i'}{t_i'} x^i, \quad s_i', t_i' \text{ are integers such that } (s_i', t_i') = 1.$$

Let, $\epsilon = \text{lcm}(t_0, ..., t_n)$ and $\epsilon' = \text{lcm}(t_0', ..., t_m')$ and assume that the epsilons are not units. The polynomials ϵg and $\epsilon' h$ have integral coefficients. They are also primitive, since, let p be a common prime divisor of the coefficients of ϵg. Choose a denominator t_a such that every prime power of p which divides a denominator t_b divides t_a. Then, $\left(\frac{\epsilon s_a}{t_a}, p\right) = (s_a, p) = 1$, contradiction. Hence, ϵg is primitive and by symmetry so is $\epsilon' h$. But, $(\epsilon g)(\epsilon' h) = (\epsilon\epsilon')gh = (\epsilon\epsilon')f$ implies that $(\epsilon g)(\epsilon' h)$ is not primitive. This contradicts with Gauss' Lemma for the pair ϵg and $\epsilon' h$.

Theorem 2.2.1 The cyclotomic polynomial Φ_n, $n \geq 1$, is irreducible in the field of rational numbers.

Proof : Equivalently, if f is a non-trivial irreducible factor of Φ_n in $\mathbb{Q}[x]$ then the roots of Φ_n are roots of f. Assume, without loss of generality, that f is monic. Let ζ be root of f. It suffices to show that ζ^m is a root of f whenever m is a positive integer relatively prime to n. We use induction on the total number $\nu(m)$ of prime factors of m.

We begin with the case $\nu(m) = 1$ i.e $m = p$, where p is a prime number relatively prime to n. As, $f \mid \Phi_n$ and $\Phi_n \mid x^n - 1$ it follows that there exists a polynomial $g \in \mathbb{Q}[x]$ such that

$$x^n - 1 = fg \tag{1}$$

Assume, contrary to the claim, that ζ^p is not a zero of f. Then ζ^p is a zero of g and so ζ is a zero of $g(x^p)$. As, $f(x), g(x^p)$ have a common zero and f is irreducible it follows by Lemma 3.1.3 that f divides $g(x^p)$ hence

$$g(x^p) = f(x)h(x) \tag{2}$$

By the corollary 2.2.1 of Gauss Lemma applied to f, g and (1) and to g, h and (2) it follows that f, g and h are polynomials in $\mathbb{Z}[x]$. Therefore, f, g, h and relations (1) and (2) can be passed to $\mathbb{Z}/(p)[x]$. So, in $\mathbb{Z}/(p)[x]$,

$$\begin{aligned}
\tilde{f}\tilde{h} = \tilde{g}(x^p) &= a_0 + ... + a_i x^{pi} + ... + a_n x^{pn}, \qquad a_0, ..., a_n \in \mathbb{Z}/(p) \\
&= {a_0}^p + ... + {a_i}^p x^{pi} + ... + {a_n}^p x^{pn}, \quad \text{by Fermat's Little Theorem} \\
&= (a_0 + ... + a_i x^i + ... + a_n x^n)^p, \quad \text{by } (a_1 + ... + a_n)^p = {a_1}^p + ... + {a_n}^p \\
&= \tilde{g}(x)^p.
\end{aligned}$$

The last equality shows that $\tilde{f}$ and $\tilde{g}$ have a common non-trivial divisor δ. On the other side, $x^n - 1$ and nx^{n-1} are relatively prime in $\mathbb{Z}/(p)[x]$. But, $nx^{n-1} = \tilde{f}'\tilde{g} + \tilde{f}\tilde{g}'$ so it follows that δ divides both $x^n - 1$ and nx^{n-1}, which is a contradiction. Hence, the case $\nu = 1$ is shown. Assume that ζ^m is a root of f for all m such that $(m, n) = 1$ and $\nu(m) = k$. Let l be an integer relatively prime to n and with $k + 1$ prime factors $p_1, ..., p_{k+1}$. Then, $p_1 p_2 \cdots p_k$ is relatively prime to n and so $\omega = \zeta^{p_1 p_2 \cdots p_k}$ is a root of f by the induction hypothesis. Therefore, as ω is a primitive p-th root of unity and a root of f it follows from the case $\nu = 1$ that $\omega^{p_{k+1}}$ is a root of f.

Theorem 2.2.2 Let ω be a primitive *m-th* root of unity. If $\gcd(m, n) = 1$ then Φ_n is irreducible in $\mathbb{Q}(\omega)[x]$

Proof : Let ζ be a primitive n-th root of unity and assume that $f = a_0 + ... + a_n x^n$ is a polynomial over $\mathbb{Q}(\omega)$ with ζ as a root. The coefficients of f are polynomial expressions in ω and so there exists polynomials $a_0(y), ..., a_n(y)$ over $\mathbb{Q}$ whose evaluation at ω give the coefficients of f. Let, $F(x, y) = a_0(x) + ... + a_n(x)y^n \in \mathbb{Q}[x, y]$ then $f(x) = F(x, \omega)$ and

$f(\zeta) = F(\zeta, \omega) = 0$. The theorem would follow if $f(\zeta^k) = F(\zeta^k, \omega)$ is zero for every integer k relatively prime to n.

Let ξ_0 be a primitive mn-th root of unity. As ω and ζ are mn-th roots of unity it follows that for some positive integers ν and ν', ${\xi_0}^{\nu} = \zeta$ and ${\xi_0}^{\nu'} = \omega$. Hence, ξ_0 is a common root of the polynomials $F(x^{\nu}, x^{\nu'})$ and Φ_{mn} and as the latter is irreducible by the previous theorem it follows by Lemma 3.1.3 that $\Phi_{mn} \mid F(x^{\nu}, x^{\nu'})$. The divisibility relation implies that every primitive mn-root of unity is a root of $F(x^{\nu}, x^{\nu'})$.

As n and m are relatively prime and as ω is a primitive m-th root of unity and ζ is a primitive n-th root of unity it follows that $\omega\zeta$ is a primitive mn-th root of unity. Additionally, there exists $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Therefore, in the above paragraph we can take $\xi_0 = \omega\zeta$, $\nu = am$ and $\nu' = bn$ and we want for every integer k relatively prime to n to find a primitive mn-root of unity ξ such that the relations $\xi^{am} = \zeta^k$, $\xi^{bn} = \omega$ are satisfied. Set $\xi = \xi_0^{t_k}$, where t_k is an integer that depends on k, then, $\xi^{am} = (\omega\zeta)^{t_k am} = \zeta^{t_k am} = \zeta^{t_k}$ and $\xi^{bn} = (\omega\zeta)^{t_k bn} = \omega^{t_k bn} = \omega^{t_k}$. By taking, $t_k = amk + bn$ we see that $\zeta^{t_k} = \zeta^k$ and $\omega^{t_k} = \omega$ and hence we have only to check that $\xi_0^{t_k}$ is a primitive mn-th root i.e that t_k is relatively prime to mn. But, $t_k = k + nb(1 - k)$ so if δ is a non-trivial divisor of both t_k and n then δ would divide k, contradiction, therefore $(m, t_k) = 1$. Also, $t_k = am(k - 1) + 1$ and so t_k is relatively prime to m too.

It follows from Theorem 2.2.2 that for a prime number p the p-th cyclotomic polynomial $\Phi_p(x)$ over $\mathbb{Q}(\omega)$, where ω is a primitive $(p-1)$-th root of unity, is irreducible. Therefore, letting ζ be a root of $\Phi_p(x)$ it follows naturally that (see Corollary 1.1.1) a basis for $\mathbb{Q}(\zeta, \omega)$ as a vector space over $\mathbb{Q}(\omega)$ is given by $\zeta, \zeta^2, ..., \zeta^{p-1}$.

Now, let a be a primitive root mod p (see Appendix) and set $\zeta_i = \zeta^{a^i}$ for $0 \leq i \leq p - 2$. The theorem that follows extends the cyclic permutation $\zeta_0 \mapsto \zeta_1 \mapsto ... \mapsto \zeta_{p-2}$ of the roots of Φ_p to a map defined on $\mathbb{Q}(\zeta, \omega)$. This map is a field automorphism.

Definition 2.2.1 A field isomorphism from a field to itself is called a field automorphism.

Proposition 2.2.1 The map $\alpha : \mathbb{Q}(\zeta, \omega) \to \mathbb{Q}(\zeta, \omega)$ given by

$$\lambda_0\zeta_0 + \lambda_1\zeta_1 + ... + \lambda_{p-3}\zeta_{p-3} + \lambda_{p-2}\zeta_{p-2} \mapsto \lambda_0\zeta_1 + \lambda_1\zeta_2 + ... + \lambda_{p-3}\zeta_{p-3} + \lambda_{p-2}\zeta_0$$

is a field automomorphism. Moreover, its restriction to the subfield $\mathbb{Q}(\omega)$ is the identity, i.e $\alpha(x) = x$ for $x \in \mathbb{Q}(\omega)$.

Proof : To begin with observe that $\zeta_0, ..., \zeta_{p-2}$ is a basis for the $\mathbb{Q}(\omega)$-vector space $\mathbb{Q}(\zeta, \omega)$ and that the map α is well-defined. It is also injective, since if

the images of two elements under α are equal then their coeffiecients in terms of the basis elements are equal. It is the identity on $\mathbb{Q}(\omega)$: let $x \in \mathbb{Q}(\omega)$ then,

$$\alpha(x) = \alpha\big((-x)\zeta_0 + ... + (-x)\zeta_{p-2}\big) = (-x)\zeta_1 + ... + (-x)\zeta_0 = x$$

It is straightforward to check that $\alpha(x+y) = \alpha(x)+\alpha(y)$ for all $x, y \in \mathbb{Q}(\zeta, \omega)$ and also that $\alpha(y_0 x) = y_0\alpha(x)$ for all $x \in \mathbb{Q}(\zeta, \omega)$ and $y_0 \in \mathbb{Q}(\omega)$.

Finally, we want $\alpha(xy) = \alpha(x)\alpha(y)$ for all $x, y \in \mathbb{Q}(\zeta, \omega)$. Therefore, let $x = \sum_{i=0}^{p-2} \lambda_i\zeta_i$ and $y = \sum_{i=0}^{p-2} \lambda_i{}'\zeta_i$ and assume for the moment that $\alpha(\zeta_i\zeta_j) = \alpha(\zeta_i)\alpha(\zeta_j)$.

$$\alpha(xy) = \alpha\bigg(\sum_{i=0}^{p-2}\sum_{j=0}^{p-2} \lambda_i\lambda_j{}'\zeta_i\zeta_j\bigg) = \sum_{i=0}^{p-2}\sum_{j=0}^{p-2} \lambda_i\lambda_j{}'\alpha(\zeta_i\zeta_j) = \sum_{i=0}^{p-2}\sum_{j=0}^{p-2} \lambda_i\lambda_j{}'\alpha(\zeta_i)\alpha(\zeta_j)$$
$$= \alpha(x)\alpha(y)$$

By definition $\forall\ i,\ 0 \le i \le p-2 : \alpha(\zeta_i) = \zeta_{i+1} = \zeta^a$. Let $\zeta_{p-1} = 1$ then for i, j between 0 and $p-2$ we have that $\zeta_i\zeta_j = \zeta_k$ for some integer $k :\ 1 \le k \le p-1$. But, $\alpha(\zeta_i\zeta_j) = \big(\zeta_i\zeta_j\big)^a = {\zeta_i}^a{\zeta_j}^a = \alpha(\zeta_i)\alpha(\zeta_j)$.

Now, let ω be a primitive (p-1)-th root of unity and consider the Lagrange resolvent (which can also be defined for roots having fixed values)

$$t_\omega = \zeta_0 + \omega\zeta_1 + ... + \omega^{p-2}\zeta_{p-2}$$

Proposition 2.2.2 The (p-1)-th power of t_ω is an element in $\mathbb{Q}(\omega)$, i.e ${t_\omega}^{p-1} \in \mathbb{Q}(\omega)$.

Proof : Since $\zeta_0, ..., \zeta_{p-2}$ is a basis for the $\mathbb{Q}(\omega)$-vector space $\mathbb{Q}(\zeta, \omega)$ there exist elements $\lambda_0, ..., \lambda_{p-2}$ in $\mathbb{Q}(\omega)$ such that ${t_\omega}^{p-1} = \lambda_0\zeta_0 + ... + \lambda_{p-2}\zeta_{p-2}$. Now, let α be the automorphism of $\mathbb{Q}(\zeta, \omega)$ of the previous theorem then

$$\alpha(t_\omega) = \zeta_1 + \omega\zeta_2 + ... + \omega^{p-3}\zeta_{p-2} + \omega^{p-2}\zeta_0 = \omega^{-1}t_\omega.$$

Therefore, $\alpha({t_\omega}^{p-1}) = \alpha(t_\omega)^{p-1} = (\omega^{-1}t_\omega)^{p-1} = {t_\omega}^{p-1}$. Hence,

$$p{t_\omega}^{p-1} = \sum_{k=1}^{p-1} \alpha^k({t_\omega}^{p-1}) = (\lambda_0 + ... + \lambda_{p-2})(\zeta_0 + ... + \zeta_{p-2}) = -\lambda_0 - ... - \lambda_{p-2}$$

But, $-\lambda_0 - ... - \lambda_{p-2}$ is an element in $\mathbb{Q}(\omega)$ and so is ${t_\omega}^{p-1}$.

Remark : The above proposition holds for any field F of characteristic zero. More specifically, let F' be a subfield of F isomorphic to $\mathbb{Q}$, ζ' a primitive p-th root of unity and ω' a primitive (p-1)-th root of unity of F'. Then the isomophism between F' and $\mathbb{Q}$ extends to an isomorphism between $F'(\omega', \zeta')$ and $\mathbb{Q}(\omega, \zeta)$ where ω' is mapped to ω and ζ' is mapped to ζ. Hence, if we arrange the p-th roots of unity as before and treat the Lagrange resolvent $t_{\omega'} = \zeta'_0 + \omega'\zeta'_1 + ... + \omega'^{p-2}\zeta'_{p-2}$ over $F'(\omega', \zeta')$ it should be an element in $F'(\omega')$ due to the previous proposition and to the above isomorphism.

Theorem 2.2.3 The n-th roots of unity, $n \geq 1$, of a field F lie in a pure radical extension of F.

Proof : For a 1-th root of unity the proposition is true. Suppose that for an arbitary field and for any k smaller than n the k-th roots of unity of F lie in a pure radical extension of F. Now, let ξ be a primitive n-th root of unity. If n is composite write $n = n_1 n_2$ for some $n_1, n_2 \in \mathbb{N} \setminus \{1\}$. Application of the induction hypothesis (twice) allows one to argue as follows: as ξ^{n_1} is a n_2-th root of unity there is a pr-extension E_1 of F containing ξ^{n_1} and there is a *pr*-extension E_2 of E_1 containing a primitive n_2-th root of unity. Since $\xi^{n_2} \in E_2$ Proposition 1.2.2 implies that there is a pr-extension E_3 of E_2 containing ξ. But, then E_3 is a pr-extension of F containing ξ. If $n = p$ is prime let ζ be a primitive p-th root of unity and ω a primitive (p-1)-th root of unity. By the induction hypothesis there is a pr-extension K_1 of F containing ω we get then $t_\omega^{p-1} \in K_1$ by the above proposition and remark. Hence it follows by proposition 1.2.2 that $K_2 = K_1(\{t_\omega : \omega \text{ is a (p-1)-th root of unity}\})$ is a pr-extension of F. And as ζ can be rationally expressed in terms of the t_ω's (see formula 2.1.2) the result follows.

Corollary 2.2.2 A polynomial f is solvable over a field F iff its roots lie in a pure radical extension of F.

Proof : By definition f is solvable over F if the roots $a, b, c, ...$ lie in a radical extension E of F. That is there exist intermediate fields $L_1, ..., L_n$ such that $F = L_0 \subseteq L_1 \subseteq ... \subseteq L_{n-1} = L_n = E$ and $L_{i+1} = L_i(a_i)$ where ${a_i}^{p'_i} \in L_i$ and p'_i is prime or 1 for all $i = 0, ..., n-1$. Let $m = \text{lcm}(p'_1, ..., p'_{n-1})$ and let ζ be a primitive m-th root of unity. By Theorem 2.2.3 there is an extension field F' of F containing ζ and intermediate fields $F_1, ..., F_{m-1}$ such that (i) $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{m-1} \subseteq F_m = F'$,
(ii) $F_{i+1} = F_i(\alpha_i)$ where ${\alpha_i}^{p_i} \in F_i$ and p_i is prime,
(iii) $x^{p_i} - {\alpha_i}^{p_i}$ is irreducible over F_i and
(iv) F_i contains a primitive p_i-th root of unity for all $i = 0, ..., m-1$.

Define now $F_{m+i} = L_i(\alpha_1, ..., \alpha_{m-1})$ for $i = 1, ..., n$ and $\alpha_{m+i} = a_i$ and $p_{m+i} = p'_i$ for $i = 0, ..., n-1$ to get a chain of fields

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_{m-1} \subseteq F_m \subseteq F_{m+1} \subseteq ... \subseteq F_{m+n-1} \subseteq F_{m+n}.$$

Clearly $F_{i+1} = F_i(\alpha_i{}^{p_i})$ where $\alpha_i{}^{p_i} \in F_i$ and p_i is prime holds for all $i = 0, ..., m+n-1$. Since each F_i contains a primitive p_i-th root of unity it follows by Lemma 1.2.1 that either $x^{p_i} - \alpha_i{}^{p_i}$ is irreducible over F_i or $F_i = F_{i+1}$. Therefore by removing fields in the above chain that possibly coincide with its predecessors we obtain that F_{m+n} is a pure radical extension of F.

3 Galois' Theory

In this chapter we try to follow the road created by Évariste Galois.

$\circ$

3.1 The Galois resolvent

Let f be a polynomial in $F[X]$ with n distinct roots $a, b, c, ...$:

Lemma 3.1.1. There is an element V in $F(a, b, c, ...)$ that assumes $n!$ distinct values when the roots are permuted. Moreover, the element can be chosen as $V = Aa + Bb + Cc...$ where $A, B, C, ...$ are integers.

Proof: The nonzero polynomial in x over the field $F(a, b, c, ...)$

$$P = \prod_{\mu,\mu' \in S_n \ \mu \neq \mu'} (\mu(a) - \mu'(a) + (\mu(b) - \mu'(b))x + (\mu(c) - \mu'(c))x^2 + ...)$$

has at most as many roots as its degree. Let n_0 be an integer which is not a root of P then $V = 1 \cdot a + n_0 \cdot b + n_0^2 \cdot c + ...$ is the required element.

Lemma 3.1.2 If an elment V is chosen according to the previous lemma, that is, let $\phi(a, b, c, ...) = V$ for some polynomial ϕ over F in n variables. Then the roots $a, b, c, ...$ lie in the extension field $F(V)$.

Claim 3.1.1 Let $z \in F[x_1, x_2, ..., x_n]$ i.e z is a polynomial over F in n variables. If it is symmetric in $x_2, ..., x_n$ then it is also a polynomial in $F[x_1, \sigma_1, ..., \sigma_n]$ where $\sigma_1, ..., \sigma_n$ are the elementary symmetric polynomials in $x_1, ..., x_n$.

Proof: Firstly, let us express the elementary symmetric polynomials $\tau_1, \tau_2, ..., \tau_{n-1}$ in $x_2, ..., x_n$ in terms of x_1 and the elementary symmetric polynomials $\sigma_1, \sigma_2, ..., \sigma_n$ in $x_1, x_2, ..., x_n$. The relations follow by observing that

$$\frac{(x - x_1)(x - x_2) \cdots (x - x_n)}{x - x_1} = x^{n-1} - \tau_1 x^{n-2} + ... + (-1)^{n-2}\tau_{n-2}x + (-1)^{n-1}\tau_{n-1}.$$

Multiplying $x - x_1$ to both sides of the above equation and equating coefficients we obtain the following realtions $\tau_1 = \sigma_1 - x_1, \tau_2 = \sigma_2 - \sigma_1 x_1 + x_1^2, \ ... \ , \tau_{n-1} = \sigma_{n-1} - \sigma_{n-2}x_1 + ... + (-1)^{n-1}x_1^{n-1}$. Now, view z as a polynomial in $F[x_1][x_2, ..., x_n]$ i.e as a polynomial over the ring $F[x_1]$ and in the variables $x_2, ..., x_n$ Since it is symmetric in $x_2, ..., x_n$ by the fundamental theorem of symmetric polynomials it lies in $F[x_1][\tau_1, ..., \tau_{n-1}]$. But, $\tau_1, ..., \tau_{n-1}$ are polynomials in $x_1, \sigma_1, ..., \sigma_{n-1}$ hence it becomes clear that

$z \in F[x_1][\sigma_1, ..., \sigma_n]$ and thus the result follows.

Proof of Lemma 3.1.2: Let $\alpha, \beta, \gamma, ...$ be n variables and consider the polynomial

$$P = \prod_{\mu \in S_n, \mu(\alpha)=\alpha} (V - \phi(\alpha, \mu(\beta), \mu(\gamma), ...)) \tag{3.1}$$

in n variables over $F(V)$. It is symmetric in the variables $\beta, \gamma, ...$ and so by Claim 3.1.1 it can by expressed as a polynomial in α and in the elementary symmetric polynomials $\sigma_1, \sigma_2, ...$ in the variables $\alpha, \beta, \gamma, ..$, hence $P = P(\alpha, \sigma_1, \sigma_2, ...)$. Now, if the $\sigma_1, \sigma_2, ...$ are given the values of the coefficients of f - σ_1 is equaled to the coefficient of the nth power of x, σ_2 is equaled to the coefficient of the $(n-1)$-th power of x, e.tc ... - and α is still considered as an indeterminate in the above expression for P then a polynomial in one variable, namely in α, over $F(V)$ is obtained and we denote it by $P'(\alpha)$. The evaluation of the $\sigma_1, \sigma_2, ...$ in the manner described and α at a distributes to $\beta, \gamma, ...$ the values of the roots $b, c, ...$. Hence, by choosing for example $\beta = b, \gamma = c, ...$ it is seen by (3.1) that a is a root of P'. To see that P' does not have any other common root with f, suppose without loss of generality that b is a root. Then $P'(b) = 0$ and hence we have evaluated α at b and again $\beta, \gamma, \delta ...$ are found among the roots $a, c, d, ...$ and without loss of generality one can put $\beta = a, \gamma = c, \delta = d$ ... . So by (3.1) one must have $V = \phi(b, \mu(a), \mu(c), ...)$ for some permutation μ fixing b, but this contradicts the way that V was chosen. So P' and f are two polynomials in $F(V)[x]$ that have only the root a in common. This implies that their greatest common divisor is $x - a$ over $F(V)[x]$ and hence $a \in F(V)$. The choice of the root was arbitary hence all the roots lie in $F(V)$.

Corollary 3.1.1 There exists an element V which is a solution of some polynomial Ω over F and is such that $F(a, b, c, ...) = F(V)$.

Proof: The existence of an element such that $F(a, b, c, ...) = F(V)$ follows immediately from Lemma 3.1.1 and Lemma 3.1.2. Let V be chosen as $V = Aa + Bb + Cc + ...$ for some integers $A, B, C, ...$. The polynomial

$$\Omega = \prod_{\mu \in S_n} (x - A\mu(a) - B\mu(b) - C\mu(c) - ...)$$

has coefficients which are symmetric in the roots $a, b, c, ...$ hence by the fundamental theorem of symmetric polynomials they can be expressed in the coefficients of f, so Ω is a polynomial in $F[x]$.

An element V which has the properties of Corollary 3.1.1 will be called a Galois resolvent for the polynomial f over F.

Corollary 3.1.2 If V and V' are Galois resolvents for f over F then $F(V) = F(V')$.

Proof: The use of Corollary 3.1.1 twice yields the statement in question.

Naturally, $F[V] = \{f(V)/g(V); f, g \in F[x], g(V) \neq 0\}$ i.e every element in $F[V]$ can be rationally expressed in terms of V and elements in F. By Lemma 3.1.2 for a and any other root of f there exists a rational function θ_o over F such that $a = \theta_o(V)$. But, as the next corollary will show the role of θ_0 can be played by a polynomial in $F[x]$(see also Proposition 1.1.2).

Corollary 3.1.3 Let Π be the minimal polyomial of V say of degree d. Then every element in $F(V)$ can be written as $a_0 + a_1V + ... + a_{d-1}V^{d-1}$, where $a_o, ..., a_{d-1} \in F$.

Proof: If an element can be polynomially expressed in terms of V and elements in F then it can be put in the desired form. To see this, let $z = a_0 + a_1V + ... + a_nV^n$ where $a_i \in F$. If $n < d$ there is nothing to prove otherwise take V^d and and use the fact that V is a root of Π in order to see that it can be put in the desired form. Proceeding inductively we can see that any power of V can be so expressed and so in turn the element z. To finish $1/g(V)$ must be given a polynomial expression. Let $V_2, ..., V_d$ be the other roots of of Π then $1/g(V) = \dfrac{\prod_{i=2}^{d} g(V_i)}{g(V)\prod_{i=2}^{d} g(V_i)}$. The denominator of the right side is symmetric in the roots of Π hence it can be polynomially expressed in the coefficients of Π and elements in F. The numerator is symmetric in the roots $V_2, ..., V_d$ and so by Claim 3.1.1 can be polynomially expressed in terms of V, the coefficients of Π and elements in F. But the coefficients of Π are elements in F and for this reason the denominator is an element in F and the numerator is a polynomial expression in V and elements in F.

So for a there exists a polynomial $\theta \in F[x]$ such that $a = \theta(V)$. Furthemore, let Π be the minimal polynomial of V and V' a root of Π distinct from V. Before proving that $\theta(V')$ is a root of Π let us recall an important lemma which will be used very frequently.

Lemma 3.1.3 Let $z(x), w(x)$ be polynomials over a field with a common zero ρ. If $z(x)$ is irreducible then it divides $w(x)$.

Proof: As z is irreducible their greatest common divisor d is 1 or z(up

to constant multiples) and d can be written as $d = z_1 z + w_1 w$ for some polynomials w_1, w_2. It follows by plugging in ρ in the above expression for d that 1 cannot be their greatest common divisor hence z is.

Lemma 3.1.4 Let V' be a root of Π distinct from V. Let r be a root of f polynomially expressed in terms of V that is $r = \theta(V)$ for some $\theta \in F[x]$. Then $\theta(V')$ is also a root of f.

Proof: The two polynomials $\Pi(x)$ and $f(\theta(x))$ over F have V as a common root. Since $\Pi(x)$ is irreducible it follows by Lemma 3.2.3 that it divides $f(\theta(x))$ which implies that all the roots of $\Pi(x)$ are roots of $f(\theta(x))$.

Let θ and θ' be two polynomials over F and let $\theta(V), \theta'(V), \theta(V')$ and $\theta'(V')$ be roots of f. If $\theta(V)$ is not equal to $\theta'(V)$ then $\theta(V')$ is not equal to $\theta'(V')$. Since otherwise if V' is a root of $\theta(x) - \theta'(x)$ then it is divisible by $\Pi(x)$ and so by Lemma 3.1.3 it follows that V is a root of $\theta - \theta'$, contradiction. It will now be possible to associate to each root of Π an arrangement of the roots $a, b, c, \ldots \ldots$.

3.2 The Galois group

Definitions Let $a, b, c, \ldots$ be n elements. There are $n!$ bijective maps from $\{1, 2, 3, \ldots, n\}$ to $\{a, b, c, \ldots\}$ and they are called arrangements. Each map α can be represented as an ordered list, that is if α is given by $1 \mapsto b$, $2 \mapsto a$, $3 \mapsto c$ then the associated list is *bac*. Given two arrangements α and α' there is a rule which when applied on α gives α'. This rule which is a map from and to $\{a, b, c, \ldots, \}$, namely $\alpha' \circ \alpha^{-1}$, is called the permutation induced from α and α'. Given now a subset A from the set of $n!$ arrangements of n letters $a, b, c, \ldots.$, one can pick a reference arrangement $\alpha \in A$ and for each arrangement $\alpha' \in A$ single out the permutation that transforms α to α'.

$\circ$

Let f be a monic polynomial in $F[X]$ with n distinct roots $a, b, c, \ldots$ and let V be a Galois resolvent for f over F with minimal polynomial Π over F. Denote by $V_2, V_3, \ldots, V_d$ the rest of the roots of Π and set $V = V_1$:

As shown in the previous section there exists polynomials $\theta_1, \theta_2, \ldots \theta_n$ over F such that $\theta_1(V) = a, \theta_2(V) = b, \ldots$. It follows from Lemma 3.1.4 in the same section that $\theta_i(Vj)$ is one of the roots $a, b, c, \ldots$ and $\theta_i(Vj) \neq \theta_{i'}(Vj)$ for all i, i', j such that $1 \leq j \leq d$, $1 \leq i, i' \leq n$ where $i \neq i'$. Hence, by writing the n distinct elements $\theta_1(V_j), \theta_2(V_j), \ldots, \theta_n(V_j)$ in the form of an ordered list

$$(Vj) \qquad \theta_1(V_j)\theta_2(V_j) \ ... \ \theta_n(V_j)$$

an arrangement of the roots $a, b, c, ...$ is obtained. The set of all arrangements $\Sigma = \{\theta_1(V_j)\theta_2(V_j) \ ... \ \theta_n(V_j)\}_{j=1}^{d}$ can be represented in the table form

$$\begin{array}{ll} (V_1) & \theta_1(V_1)\theta_2(V_1) \ ... \ \theta_n(V_1) \\ (V_2) & \theta_1(V_2)\theta_2(V_2) \ ... \ \theta_n(V_2) \\ & \quad . \\ & \quad . \\ & \quad . \\ (V_d) & \theta_1(V_d)\theta_2(V_d) \ ... \ \theta_n(V_d). \end{array}$$

Consider (V_1) as a reference arrangement then there are d distinct permutations of the roots $a, b, c, ...$ that transform (V_1) to any other arrangement in Σ. Namely, for $j = 1, 2, ..., d$ they are given by

$$\mu_j : \theta_1(V_1) \mapsto \theta_1(Vj), \ \theta_2(V_1) \mapsto \theta_2(Vj), \ ... \ , \ \theta_n(V_1) \mapsto \theta_n(Vj).$$

The set of permutations so obtained will be called the Galois group of (of permutations) f over F and we denote by G_F. The permutations in G_F have the following double property:

Theorem 3.2.1

(1) Every polynomial expression in the roots unaltered by the permutations of G_F belongs to F. That is, if M is a polynomial over F in n variables such that $M(\mu(a), \mu(b), \ ... \ ) = M(a, b, \ ... \ )$ for all permutations $\mu \in G_F$ then $M(a, b, \ ... \ )$ is an element in F.

(2) Every polynomial expression in the roots lying in F remains unaltered by the permutations of G_F. That is, if $M(a, b, c, \ ... \ )$ is an element in F then $M(\mu(a), \mu(b), \ ... \ ) = M(a, b, \ ... \ )$ for for all permutations $\mu \in G_F$.

Proof : (1) Consider the polynomial $M(\theta_1(x), \theta_2(x), \ ... \ ) = M'(x)$ over F. By, assumption

$M(\theta_1(V_j), \theta_2(V_j), \ ... \ ) = M(a, b, \ ... \ )$ for $j = 1, 2, \ ... \ , d.$

So, $M(a, b, \ ... \ ) = \frac{1}{d} \sum_{j=1}^{d} M'(V_j).$

The polynomial $p = \sum_{j=1}^{d} M'(x_j)$ over F in n indeterminates $x_1, x_2, ..., x_n$ is symmetric. Thus p is a polynomial in $F[\sigma_1, ..., \sigma_n]$ where $\sigma_1, \sigma_2, \ ..., \sigma_n$ are the elementary symmetric polynomials in the variables $x_1, x_2, ..., x_n$. But when $x_1 = V_1, x_2 = V_2, \ ..., x_d = V_d$ then $\sigma_1, \sigma_2, \ ..., \sigma_n$ are equal to the coefficients of Π. So, $\sum_{j=1}^{m} M'(V_j)$ can be polynomially expressed in terms of the coefficients of Π, but these lie in F hence $M(a, b, \ ... \ )$ lies in F too.

(2) The polynomial $M''(x) = M(\theta_1(x), \theta_2(x), \ ... \ ) - M(a, b, \ ... \ )$ over F has V_1 among its roots. But, V_1 is a root of Π which is an irreducible polynonial and so by Lemma 3.1.3 Π divides M''. This implies that the roots of Π are roots of M'' and so $M(\theta_1(V_j), \theta_2(V_j), \ ... \ ) = M(a, b, \ ... \ )$.

Remark: Every rational expression of the roots $a, b, ...$ over F can be transformed to a polynomial expression in $a, b, ...$ over F, since if g is a polynomial in n variables over F then $1/g(a, b, ...) = A/\prod_{\mu \in S_n} g(\mu(a), \mu(b), ...)$ and so A is a polynomial expression in $a, b, c, ...$ over F and the denominator is an element in F by the fundamental theorem of symmetric polynomials. Hence, Theorem 3.2.1 implies that every rational expression in the roots is unaltered by the permutations of G_F if and only if it lies in F.

Suppose now that an arbitatry permutation μ of the roots $a, b, c, ...$ is given and which is such that every rational expression in the roots is unaltered by it if and only if it is an element in F. It will be shown that μ is a permutaion of the Galois group of f over F. It will also be proved that G_F has a group structure and in order to to reveal it one needs a fact that is of technical value for the moment, but actually the starting point in the modern formulation of Galois Theory. It will be shown that the permutations of G_F can be extended to the field $F(a, b, \ ... \ )$ where they become automorphisms keeping the base field F fixed.

Corollary 3.2.1 For every permutation μ of the roots $a, b, c, ...$ such that $M(a, b, ...) = M(\mu(a), \mu(b), ...)$ if and only if $M(a, b, ...) \in F$ the map $\tilde{\mu}(M(a, b, \ ... \ )) = M(\mu(a), \mu(b), \ ... \ )$ defined on the field $F(a, b, \ ... \ )$ is an automorphism and $\tilde{\mu}(x) = x$ for $x \in F$.

Proof: First of all it has to be shown that $\tilde{\mu}$ is a map. Therefore, suppose that $M(a, b, c, ...) = M'(a, b, c, ...)$ for some polynomials M, M' in $F[x_1, ..., x_n]$. As $M(a, b, c...) - M'(a, b, c...) = 0 \in F$ and μ fixes the elements of F it follows that $\tilde{\mu}$ is well-defined. It is not difficult to see that it preserves

products and sums, that it is one-to-one and bijective and that it is the identity on F.

Remark: In the next sections of this chapter we will not distiguish between μ and $\tilde{\mu}$. This is possible for the next propositions too, but we ought to be more careful in the beginning.

Lemma 3.2.1 Let μ be a permutation of the roots $a, b, c...$. If $\tilde{\mu}(V_1)$ is one of the roots of Π then $\mu \in G_F$.

Proof: It follows directly from the definition of the Galois group and from corrolary 3.2.1 that μ is the permutation that changes the arrangement (V_1) to (V_j) for some j between 1 and d such that $V_j = \tilde{\mu}(V_1)$.

Corollary 3.2.2 G_F contains all permutations μ of the roots $a, b, c, ...$ having the property $M(a, b, ...) = M(\mu(a), \mu(b), ...)$ iff $M(a, b, c, ...) \in F$.

Proof: Let μ be a permutation that has this property. Then $\tilde{\mu}(V_1)$ is a root of Π, hence by Lemma 3.2.1 μ is a permutation in G_F.

Corollary 3.2.3 The Galois group G_F is a group under the operation of map composition.

Proof: One can check that all the axioms for a group are satisfied. But, since G_F is a subset of the symmetric group it suffices to verify that it is closed under map composition. Let $\mu, \nu \in G_F$ then $(\widetilde{\mu\nu})(V_1)$ is a root of Π hence by Lemma 3.2.1 $\mu\nu$ is in G_F.

Now, it has been shown how from a polynomial f with n distinct roots a subgroup of the symmetric group can be associated. The choice of a Galois resolvent played the initial role and by Corollary 3.2.2 the Galois group G_F is independent of the choice.

Two examples of Galois groups

(α) We claim that the Galois group of the polynomial $x^n - 1$ over $\mathbb{Q}$ is (isomorphic to) the group $U(\mathbb{Z}/(n))$ of invertible elements in $\mathbb{Z}/(n)$. In this case, it seems that a natural choice of a Galois resolvent is a primitive n-th root of unity ρ, but we do not need to view ρ as a Galois resolvent in order to determine G_F (compare wth [4]). The minimal polynomial of ρ is the n-th cyclotomic polynomial whose roots are of the form ρ^m where m is an integer relatively prime to n. Each permutation $\mu \in G_F$ maps ρ to a primitive n-th root of unity and it is determined by the image of ρ, since $\tilde{\mu}(\Phi_n(\rho)) = \Phi_n(\mu(\rho)) = 0$ hence $\mu(\rho) = \rho^m$ for some m such that $(m, n) = 1$.

Therefore, we get a map ϕ from G_F to $U(\mathbb{Z}/(n))$ by letting $\phi(\mu) = [m]$. It is clear that ϕ is an injective group homomorphism and the from the next lemma it follows that ϕ is a group isomorphism.

Lemma 3.2.2 If a polynomial f over a field F of degree one and higher is irreducible then for all roots α, β of f there is a permutation $\mu \in G_F$ such that $\mu(\alpha) = \beta$.

Proof: Assume that f is irreducible and that there is no permutation in the Galois group of f that maps α to β. Let $\beta_1, ..., \beta_n$ be distinct roots of f and such that if $\mu \in G_F$ then $\mu(a)$ is one of the β_i's. The coefficients of the polynomial $g(x) = \prod_{i=1}^{n}(x - \beta_i)$ are left fixed by the permutations of G_F hence g is a polynomial over F with α as a root and of degree less than f, contradiction.

In the case p is prime the group $U(\mathbb{Z}/(p))$ is generated by a single element so the Galois group of $x^p - 1$ is cyclic of order $p - 1$.

(β) The Galois group of the general polynomial $f(x) = \prod_{i=1}^{n}(x - x_i)$ over $F = \mathbb{Q}(\sigma_1, ..., \sigma_n)$ where $\sigma_1, ..., \sigma_n$ are the elementary symmetric polynomials in the variables $x_1, ..., x_n$ consists of all $n!$ permutations of the roots. To see this suppose contrary that G_F is not the symmetric group S_n. Let, $g(x_1, ..., x_n) = \sum_{\mu \in G_F} \mu(x_1)\mu(x_2)^2 ... \mu(x_n)^n$, clearly, g is left invariant by the permutations of G_F. Let, ν be a permutation of the $x_1, ..., x_n$ that is not in G_F then as $\nu(x_1)\nu(x_2)^2 ... \nu(x_n)^n$ is not a term of the sum g and as the elements of the set $\left\{x_1^{n_1} x_2^{n_2} ... \ x_n^{k_n};\ n_i \in \mathbb{N} \cup \{0\}\right\}$ are linearly independent over the $\mathbb{Q}$-vector space $\mathbb{Q}(x_1, ..., x_n)$ it follows that $\nu(g) \neq g$. Hence, g is not symmetric in the variables $x_1, ..., x_n$ and so not an element in F. But, this contradicts theorem 3.2.1 from which it follows that g is an element in F since it is left invariant by the permutations of G_F.

3.3 Field extensions and Galois groups

Let f be a polynomial in $F[x]$ with n distinct roots $a, b, c, ...$. Let V be a Galois resolvent for F and G_F its Galois group. Let F' be the field obtained from F by adjunction of a root ρ of an irreducible polynomial A over F say of degree d :

The Galois resolvent V for f over F is also a Galois resolvent for f over F'. Denote by Π' the minimal polynomial of V over F'. Since V is a root of both Π and Π' and as Π' is irreducible over F' it follows that Π' divides

Π over F'.

Proposition 3.3.1 $G_{F'}$ is a subgroup of G_F.

Proof: Let $\mu \in G_{F'}$ the proposition would follow from Lemma 3.2.1 if $\mu(V)$ are among the roots of Π. But, $\mu(V)$ is a root of Π' hence a root of Π too.

Let $k = |G_F|$ =degΠ and $k' = |G_{F'}|$ =degΠ'. As $\Pi'(x) \mid \Pi(x)$ there is a polynomial P in $F(\rho)[x]$ such that $\Pi(x) = \Pi'(x)P(x)$. Hence,

$$\Pi'(x) = \Pi'(x,\rho) = x^{k'} + \sigma_1(\rho)x^{k'-1} + ... + \sigma_{k'}(\rho)$$

$$P(x) = P(x,\rho) = x^{k-k'} + \sigma'_1(\rho)x^{k-k'-1} + ... + \sigma'_{k-k'}(\rho).$$

Let $\Pi'(x,y), P(x,y)$ be the polynomials in $F[x,y]$ given by

$$\Pi'(x,y) = x^{k'} + \sigma_1(y)x^{k'-1} + ... + \sigma_{k'}(y)$$

$$P(x,y) = x^{k-k'} + \sigma'_1(y)x^{k-k'-1} + ... + \sigma'_{k-k'}(y),$$

where σ_i, σ'_i are polynomials in $F[y]$.

Proposition 3.3.2 $\Pi(x) = \Pi'(x,\rho')P(x,\rho')$ for any root ρ' of $A(x)$.

Proof: Let $\Pi(x) = x^k + c_1x^{k-1} + ... + c_k$ where $c_i \in F$ and take the product $\Pi'(x,y)P(x,y) = x^k + \sigma''_1(y)x^{k-1} + ... + \sigma''_k(y)$, where $\sigma''_i(y) \in F[y]$. The claim would follow if $\sigma''_i(\rho') - c_i = 0$ for any i. The polynomials $\sigma''_i(y) - c_i = 0$ and $A(y)$ have a root in common ρ, but $A(y)$ is irreducible over F hence by Lemma 3.2.3 the roots of $A(y)$ are roots of $\sigma''_i(y) - c_i$.

Theorem 3.3.2 $|G_F|/|G_{F'}| \mid d$

Proof: Let now $\rho = \rho_1, \rho_2, ..., \rho_d$ be the roots of A. By Proposition 3.3.2 it follows that

$\Pi(x)^d = \prod_{j=1}^{d} \Pi'(x,\rho_j) \prod_{j=1}^{d} P(x,\rho_j)$.

$P'(x) = \prod_{j=1}^{d} \Pi'(x,\rho_j)$ is symmetric in $\rho_1, \rho_2, ..., \rho_d$. Hence by the fundamental theorem of symmetric polynomials it is an element in $F(\sigma_1, \sigma_2, ..., \sigma_d)[x]$ where $\sigma_1, \sigma_2, ..., \sigma_d$ are the elementary symmetric polynomials in $\rho_1, \rho_2, ..., \rho_d$. But $\sigma_1, \sigma_2, ..., \sigma_d$ are the coefficients of A hence P'

is a polynomial in $F[x]$. Since $P' \mid \Pi^d$ over F and Π is irreducible it follows that $P' = \Pi^l$ for some integer l between 1 and d. Finally, $\deg\Pi \cdot l = \deg P' = \mathrm{d} \cdot \deg\Pi'$.

Notation : When we write $N \trianglelefteq G$ we will mean that N is a normal subgroup of G.

Theorem 3.3.3 Suppose now that all roots of A are adjoined to F, $F(\rho_1, \rho_2, ..., \rho_d) = F''$. Then the Galois group of f over F'' is a normal subgroup of the Galois group of f over F, i.e $G_{F''} \trianglelefteq G_F$.

Proof: V the Galois resolvent for f over F is also a Galois resolvent for f over F''. Let Π'' be the minimal polynomial for V over F''. For any permutation $\mu \in G_{F''}$ choose $\theta_1(V)\theta_2(V)...\theta_n(V)$ as reference arrangement. Then $\mu : \theta_i(V) \mapsto \theta_i(V')$ for some root V' of Π'' and $i = 1, ..., n$. Also, if $\nu \in G_F$ then $\nu : \theta_i(V) \mapsto \theta_i(V'')$ for some root V'' of Π. It has to be shown that $\nu \circ \mu \circ \nu^{-1} \in G_{F''}$. Evidently, there exists a permutation μ' in G_F such that $\nu \circ \mu = \mu' \circ \nu$ and normality would follow if μ' belongs to $G_{F''}$. But, $V'' = \nu(V)$ is a Galois resolvent for f over F'' so if $\nu(V') = \mu'(\nu(V))$ is one of the roots of the minimal polynomial of $\nu(V)$ over F'' then Lemma 3.2.1 gives that $\mu' \in G_{F''}$.

By Corollary 3.1.1 there is an algebraic element λ over F such that $F(\rho_1, \rho_2, ..., \rho_d) = F(\lambda)$. Let Φ be the minimal polynomial for λ over F. As Π'' divides Π it follows that there is a polynomial P'' over $F(\lambda)$ such that $\Pi(x) = \Pi''(x, \lambda)P''(x, \lambda)$, where $\Pi''(x, \lambda) = \Pi''(x)$. Assume now that Φ has degree d' and $\lambda = \lambda_1, \lambda_2..., \lambda_{d'}$ are its roots and apply Proposition 3.3.2 d' times to obtain

$$\Pi(x)^{d'} = \prod_{i=1}^{d'} \Pi''(x, \lambda_i) \prod_{i=1}^{d'} P(x, \lambda_i).$$

Then since $\prod_{i=1}^{d'} \Pi''(x, \lambda_i)$ is symmetric in $\lambda_1, ..., \lambda_{d'}$ it is a polynomial in $F[x]$ and since $\Pi(x)$ is irreducible over F it follows that $\prod_{i=1}^{d'} \Pi''(x, \lambda_i) = \Pi(x)^{l'}$ for some integer l' between 1 and d'. Now, V and V' are roots of $\Pi''(x, \lambda)$ and $\nu(V)$ is a root of $\Pi''(x, \lambda_j)$ for some j. By Corollary 3.1.2 it follows that $F(\lambda) = F(\lambda_j)$ hence the polynomial $\Pi''(x, \lambda_j)$ is in $F(\lambda)[x]$ where it is also irreducible. Because if it were reducible then

$$\Pi''(x, \lambda_j) = \Psi(x, \lambda_j)\Psi'(x, \lambda_j)$$

for some polynomials Ψ and Ψ' in $F[x, y]$, where the degree of both

$\Psi(x, \lambda_j)$ and $\Psi'(x, \lambda_j)$ is greater than one. Now,

$$\Pi''(x, y) - \Psi(x, y)\Psi'(x, y) = \sigma_0(y)x^m + \sigma_1(y)x^{m-1} + ... + \sigma_m(y)$$

for some positive integer m and some polynomials σ_i over F. As λ_j is a common root of A and σ_i and as A is irreducible it follows that $\sigma_i(\lambda) = 0$ and hence that $\Pi''(x, \lambda) = \Psi(x, \lambda)\Psi'(x, \lambda)$ and so Π'' is reducible, contradiction.

Hence $\Pi''(x, \lambda_j)$ is the minimal polynomial of $\nu(V)$ and it has to be shown that it is of $\nu(V')$ too. Accordingly, $V' \in F(V)$ hence there is a polynomial η in $F[x]$ such that $V' = \eta(V)$. Since V is a common root of $\Pi''(\eta(x), \lambda)$ and $\Pi''(x, \lambda)$ and as the latter is irreducible it follows by Lemma 3.2.3 that for some polynomial of two variables Q over F the relation $\Pi''(\eta(x), \lambda) = \Pi''(x, \lambda)Q(x, \lambda)$ holds. Now, interchanging λ with an indeterminate y in the relation gives $\Pi''(\eta(x), y) = \Pi''(x, y)Q(x, y) + Q'(x, y)$ where all concerned polynomials have coefficients in F. To see that $Q'(x, \lambda_j) = 0$ observe that $Q'(x, \lambda) = 0$ and that the coefficients of Q as a polynomial over $F[y]$ are polynomials in y over F, say $c_i(y)$. But $c_i(\lambda) = 0$ and as λ is a root of the irreducible polynomial Φ over F it follows that $c_i(\lambda_j) = 0$.

Finally, it follows that $\Pi''(\eta(x), \lambda_j) = \Pi''(x, \lambda_j)Q(x, \lambda_j)$ so $\nu(V)$ is a root of $\Pi''(\eta(x), \lambda_j)$ and so $\Pi''(\eta(\nu(V)), \lambda_j) = \Pi''(\nu(V')), \lambda_j) = 0$.

Theorem 3.3.4 If an element $v \in F(a, b, c...)$ is adjoined to F the Galois group of f over $F(v)$ will consist of the permutations of G_F that leave the element invariant.

Proof: By Corollary 3.3.4 the Galois group of f over $F(v)$ contains all the permutations that leaves v invariant and as $G_{F(v)}$ is subgroup of G_F the result follows.

3.4 Galois groups and field extensions

Lemma 3.4.1 Let p be a prime and N a normal subgroup of a group G of index p. For any $g \in G$ but not in N, $g^p \in N$ and $g^k \notin N$ for $1 \leq k < p$.

Proof: The factor group G/N has prime order p. Consider the subgroup generated by an element gN that is not the identity, by Lagrange's theorem the order of this subgroup must divide the order of G therefore it follows that $(gN)^p = g^pN = N$ and $(gN)^k \neq N$ for $1 \leq k < p$.

Theorem 3.4.1 Let f be a polynomial over a field with n distinct roots $a, b, c, ...$ and G_F its Galois group. Assume that a primitive pth root of unity lies in F and that G_F has a normal subgroup N of prime index p. Then it is possible to adjoin to F a pth root of an element in F in such a way that the Galois group over the extended field coincide with N.

Proof: The existence of an element $\omega \in F(a, b, c, ...)$ with the following properties will be demonstrated:

(1) ω is not invariant under all permutations in G_F but invariant under those in N,

(2) its pth power is an element in F.

Consider the Galois group of f over $F(\omega)$. By (1) and Theorem 3.3.4 the permutations of N are elements in $G_F(\omega)$ and by (1), (2) and Theorem 3.3.2 the groups $G_F(\omega)$ and N have the same cardinality. Therefore the two groups coincide.

Let V be a Galois resolvent for f over F and Π the minimal polynomial of V over F. The polynomial $\prod_{\nu \in N}(x - \nu(V))$ cannot have all its coefficients in F because it has degree smaller than Π and Π is the minimal polynomial of V over F. Hence there is at least one coefficient θ that is altered by a permutation μ in G_F, that is, $\mu(\theta) = \theta_1 \neq \theta$. Define $\theta_k = \mu^k(\theta)$ for $k = 1, ..., p-1$ and observe that $\mu^p(\theta) = \theta$ by Lemma 3.4.1. Let ζ be a primitive pth root of unity and consider the element

$$\omega_i = \theta + \zeta^i\theta_1 + (\zeta^i)^2\theta_2 + ... + (\zeta^i)^{p-1}\theta_{p-1}, \text{ for } i = 1, ..., p-1.$$

We can assume without loss of generality that $\omega = \omega_1$ is non-zero. And this because if all the ω_i where zero then

$$0 = \sum_{i=1}^{p-1}\omega_i = (p-1)\theta + \sum_{k=1}^{p-1}\sum_{i=1}^{p-1}(\zeta^i)^k\theta_k = \sum_{k=1}^{p-1}\theta_k\sum_{i=1}^{p-1}(\zeta^k)^i = (p-1)\theta.$$

Let $\nu \in N$ by normality of N we get that for some ν_i in N the relation holds $\nu(\theta_i) = \nu(\mu^i(\theta)) = \mu^i(\nu_i(\theta))$ for $i = 1, ..., p-1$, and by the fact that the pemutations of N fixes θ we get $\nu(\theta_i) = \mu^i(\theta)$ and so

$$\nu(\omega) = \nu(\theta) + \zeta\nu(\theta_1) + ... + \zeta^{p-1}\nu(\theta_{p-1}) = \theta + \zeta\theta_1 + ... + \zeta^{p-1}\theta_{p-1} = \omega$$

Property (1) has already been shown. Additionaly,

$$\mu(\omega) = \theta_1 + \zeta\theta_2 + ... + \zeta^{p-1}\theta = \zeta^{-1}\omega \text{ and so } \mu(\omega^p) = \mu(\omega)^p = (\zeta^{-1}\omega)^p = \omega^p$$

Now, because every element in G_F can be written as $\mu^k\nu$ for some permutation $\nu \in N$ and for some integer k between one and p it follows that ω^p is fixed by the permutations in G_F. Therefore ω^p is an element in F and so property (2) holds.

3.5 Conditions for solvability

Definition 3.5.1 A group G is called solvable if there exists a chain of subgroups $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_{k-1} \trianglelefteq N_k = G$ such that the index of N_i in N_{i+1} is a prime number p_i for each $i = 0, ..., k-1$. We say that the subgroups $N_0, N_1, ..., N_{k-1}, N_k$ of G form a normal series of G.

Lemma 3.5.1 A subgroup H of a solvable group G is a solvable group.

Proof: Since the group G is solvable there exists a chain of subgroups $\{e\} \trianglelefteq N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_{k-1} \trianglelefteq N_k = G$ such that N_{i+1}/N_i has prime order p_i. Let $h \in H \cap N_i$ and $g \in H \cap N_{i+1}$ and note that since N_i is a normal subgroup of N_{i+1} it follows that $ghg^{-1} \in N_i$. Clearly, $ghg^{-1} \in H$ and hence $H \cap N_i$ is a normal subgroup of $H \cap N_{i+1}$. Now, if $H \cap N_i \neq H \cap N_{i+1}$ then there is an element $a \in N_{i+1}$ such that aN_i generates N_{i+1}/N_i. But, then $aH \cap N_i$ generates $H \cap N_{i+1}/H \cap N_i$ and it follows that the factor group $H \cap N_{i+1}/H \cap N_i$ has order p_i. Now, consider the chain of subgroups of H; $\{e\} = H \cap N_0 \subseteq H \cap N_1 \subseteq ... \subseteq H \cap N_{k-1} \subseteq H \cap N_k = H$ and we are finished after removing subgroups in the chain that are equal to its predecessors.

Proposition 3.5.1 Suppose that a polynomial f over a field F having n distinct roots $a, b, c, ...$ is solvable. Then the Galois group of f over F is a solvable group.

Proof: By Corollary 2.2.1 the roots of f lie in pure radical extension. The rest follows by Theorems 3.3.2 and 3.3.3 and by the fact that the only element of the Galois group of f over an extension field of F that contains the roots $a, b, c, ...$ is the identity permutation.

Conversely,

Proposition 3.5.2 Suppose that the Galois group of a polynomial f with n distinct roots $a, b, c, ...$ over a field F is solvable. Then f is a solvable polynomial over F.

Proof: By definition, since G_F is solvable, there is a chain of subgroups of G_F such that $G_F = N_k \supset N_{k-1} \supset ... \supset N_1 \supset N_0 = \{e\}$, N_{i+1} is a normal subgroup of N_i and the index of N_i in N_{i+1} is equal to a prime p_i, for $i = 0, 1, ..., k-1$. Let m the least common multiple of the primes p_i, $i = 0, 1, ..., k-1$ and let ζ be a primitive m-th root of unity of F. By Theorem 2.2.3 there is a pure radical extension E of F containing ζ. By Proposition 3.3.1 G_E is a subgroup of G_F hence solvable by Lemma 3.5.1. Inspection of the proof of of Lemma 3.5.1 shows that there is a normal series $\{e\} = N'_0, N'_1, ..., N'_{k-1}, N'_k = G_E$ such that N'_{i+1}/N'_i has order p_i. Now, by

Theorem 3.4.1 we can proceed as follows. Adjoin to E an element a_0 whose p_0-th power lies in E and is such that the index of $G_{E(a_0)}$ in G_E is equal to p_0. Set $E = E_0$ and $E_0(a_0) = E_1$, and continue inductively for $n = 2, ..., k-1$ by adjoining an element a_n to the field $E_{n-1}(a_{n-1}) = E_n$ whose p_n-th power is an element in E_n and is such that the index of $G_{E_n(a_n)}$ in G_{E_n} is equal to p_n. Finally, observe that a_n cannot be a p_n-th power of an element in E_n and so $x^{p_n} - a_n$ is irreducible over E_n by Lemma 1.2.1. Hence $E_{k-1}(a_{k-1})$ is a pure radical extension of E which contains the roots $a, b, c, ...$.

4 Modern Galois theory

The Galois group of permutations of a polynomial f over a field F consists of those permutations of the roots of f that leave F invariant. A permutation of G_F gives rise to an automorphism of the the splitting field of f that keeps F invariant and, clearly, each automorphism of the splitting field that leaves F invariant induces a permutation in G_F. So, for each extension field E of F that is the splitting field of a polynomial it is natural to define the group of automorphisms of E that acts on the roots of the polynomial as the elements of G_F. This leads to the definition of the Galois group of automorphisms of a field extension. In this chapter, we aim to see how the structure of the Galois group of the field extension E/F relates to the structure of the extension. Additionaly, the arguments in this section do work for fields of any characteristic.

$\circ$

4.1 Splitting fields

Definition 4.1.1 A polynomial f over a field F splits over F if it has all its roots in F. An extension E of a field F is the splitting field for a polynomial f if f splits over E but does not split over any intermediate field of the field extension E/F.

Theorem 4.1.1 A polynomial f over a field F has a splitting field. Moreover, the splitting field of f over F has finite degree over F.

Proof: For a polynomial of degree one the proposition holds true. Assume that in an arbitary field F a polynomial of degree n has a splitting field which is of finite degree over F. Let f be a polynomial of degree $n+1$ which does not split over F. By Theorem 1.1.1 there is an extension E of finite degree over F in which f has a root. So, f factors as $f = (x - e)g$ where e is some element in E and g is a polynomial of degree n in E. By induction g has a splitting field E' over $F(e)$ which is also a splitting field for f and $[E' : F(e)] < \infty$. Then E' is a splitting field of f over F and by the tower law E' is of finite degree over F.

Proposition 4.1.1 Let $i : F \to F'$ be a field isomorphism. Let also, r be a root of an irreducible polynomial f over F and r' a root of $i(f)$. Then i can be extended to an isomorphism between $F(r)$ and $F'(r')$.

Proof: The map $\phi : F(r) \to F[x]/(f)$ given by $g(a) \mapsto g(x) + (f)$ is a field isomorphism, so are the maps $\xi : F[x]/(f) \to F'[x]/(i(f))$ given by $g(x) + (f) \mapsto \phi(g(x)) + (i(f))$ and $\psi : F'[x]/(i(f)) \to F(r')$ given by

$g(x) + (i(f)) \mapsto g(b)$. Then, $\psi\xi\phi : F(r) \to F'(r')$ is the desired field isomorphism that extensds i.

The fact that follows proves the uniqueness, up to isomorphisms, of the splitting field of a given polynomial.

Theorem 4.1.2 Let $\phi : F \to F'$ be a field isomorphism. Let $p(x)$ be a polynomial in F with splitting field E and let E' be the splitting field of the polynomial $\phi(p(x))$. Let also, $r \in E$ be a root of an irreducible polynomial g over F and r' a root $\phi(g(x))$. Then there is an isomorphism $\overline{\phi}$ between E and E' that extends ϕ and such that $\overline{\phi}(r) = r'$.

Proof: For a field extension E/F of degree one the theorem is true and assume that it is true for every pair of fields (E, F) such that $[E : F]$ is smaller than n and satisfying the conditions of the theorem.

Let now E/F be an extension of degreee n and assume that p does not have all its roots in F, otherwise the theorem is clear, and choose an irreducible factor q of degree larger than one. Let r denote a root of q and r' a root of $\phi(q)$. Then by the previous proposition there is an isomorphism of fields $\phi' : F(r) \to F'(r')$ such that $\phi'(r) = r'$. By the tower law $[E : F(r)] < n$ and as E and E' are the splitting fields for f over $F(r)$ and for f' over $F'(r')$ respectively, the inductive hypothesis to the pair $(E, F(r))$ together with the field isomorphism ϕ' can be applied to show the existense of $\overline{\phi}$.

4.2 Automorpisms as group characters

Definition 4.1.1 A group character χ from a group G to the multiplicative group of a field F is a homomorphism $\chi : G \to F^*$, where $F^* = F \setminus \{0\}$.

The characters $\chi_1, ..., \chi_n$ from G to F^* are linearly independent over F if for all elements $\lambda_1, ..., \lambda_n$ in F such that $\lambda_1\chi_1(g) + ... + \lambda_n\chi_n(g) = 0$ for all $g \in G$ implies $\lambda_1 = ... = \lambda_n = 0$. $\chi_1, ..., \chi_n$ are called linearly dependent if they are not linearly independent.

Proposition 4.2.1 If $\chi_1, ..., \chi_n$ are distinct characters from G to F^* then $\chi_1, ..., \chi_n$ are linearly independent over F.

Proof: Suppose otherwise, then there exist $\lambda_1, ..., \lambda_n$ in F not all zero s.t $\lambda_1\chi_1(g) + ... + \lambda_n\chi_n(g) = 0$ for all $g \in G$. Among all n-tuples of elements in F which correspond to a relation of linear dependence of $\chi_1, ..., \chi_n$ there is one with the smallest number m of non-zero coordinates. Clearly, $m \neq 1$ and reindexing if needed one can write $(l_1, ..., l_m, 0, ..., 0)$. And so

$$l_1\chi_1(g) + ... + l_m\chi_m(g) = 0 \text{ for all } g \in G \tag{1}$$

As χ_1 and χ_m are distinct there exists $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_m(g_0)$. Now, plug in $g_0 g$ in (1) to get the equation

(2) $$l_1\chi_1(g_0)\chi_1(g) + ... + l_m\chi_m(g_0)\chi_m(g) = 0 \text{ for all } g \in G$$

and multiply (1) with $\chi_m(g_0)$ to get

(3) $$l_1\chi_m(g_0)\chi_1(g) + ... + l_m\chi_m(g_0)\chi_m(g) = 0 \text{ for all } g \in G$$

Substracting (3) from (2) we see that the n-tuple $\big(l_1(\chi_1(g_0) - \chi_m(g_0), ..., l_{m-1}(\chi_{m-1}(g_0) - \chi_{m-1}(g_0), 0, ..., 0\big)$ represents a relation of linear dependence of $\chi_1, ..., \chi_n$, contradiction.

Any automorphism of a field can be seen as a character from the multiplicative group of the field to itself.

Definition 4.2.2 Let $\alpha_1, ..., \alpha_n$ be automorphims of a field F. The fixed field of the α_i's is defined as the field $\mathcal{I}(\alpha_1, ..., \alpha_n) = \{x : \alpha_1(x) = ... = \alpha_n(x)\}$. If $G = \{\alpha_1, ..., \alpha_n\}$ forms a group, then since the identity map is in G the fixed field of G is $\mathcal{I}(G) = \{x : x = \alpha_i(x) \ \forall \ i\}$.

In the propositions and theorems that follow assume always that the degree of the extension E/F is not ∞.

Proposition 4.2.2 Let $\alpha_1, ..., \alpha_n$ be distinct automorphisms of a field E with fixed field F. Then, $n \leq [E : F]$.

Proof: Assume that the degree m of the extension E/F is strictly smaller than n and let $e_1, ..., e_m$ be a basis for E as a vector space over F. For each nonzero element e in E there exist elements $f_1, ..., f_m$ in F such that $e = f_1e_1 + ... + f_me_m$. Let $x_1, ..., x_n$ be variables and using that F is the fixed field of $\alpha_1, ..., \alpha_n$ we get,

$$x_1\alpha_1(e) + ... + x_n\alpha_n(e) = \sum_{i=1}^{n} x_i\alpha_i(\sum_{j=1}^{m} f_je_j) = \sum_{i=1}^{n} x_i \sum_{j=1}^{m} \alpha_i(f_j)\alpha_i(e_j) =$$

$$\sum_{i=1}^{n} x_i \sum_{j=1}^{m} f_j\alpha_i(e_j) = \sum_{j=1}^{m} f_j \sum_{i=1}^{n} x_i\alpha_i(e_j).$$

The m equations $\sum_{i=1}^{n} x_i\alpha_i(e_j) = 0$, where j takes values from 1 to n, determine a linear system over E which has a non-trivial solution $(\lambda_1, ..., \lambda_n)$ since it has more unknowns than equations. But, then $(\lambda_1, ..., \lambda_n)$ represents a relation of linear dependence among the distinct characters induced

by $\alpha_1, ..., \alpha_n$, a contradiction to Propostion 4.2.1.

Definition 4.2.3 Let E be an extension field of F. The Galois group of automorphisms of E/F is defined as the set of all automorphisms of E that fixes the base field F, that is, if we denote by $Av\tau(E)$ the set of field automorphisms of E then $\text{Gal}(E/F) = \{\alpha \in Av\tau(E) : \alpha(x) = x \ \forall \ x \in F\}$.

The fixed field of the Galois group of an extension E/F contains F, i.e $\mathcal{I}(\text{Gal}(E/F)) \supseteq F$, hence by the tower law and by Propostion 4.2.2 it follows that $|\text{Gal}(E/F)|$ is equal or smaller than the degree of the extension E/F.

Definition 4.2.4 A finite field extension E/F is called Galois if the condition $\mathcal{I}(\text{Gal}(E/F)) = F$ is satisfied.

Theorem 4.2.1 If $G = \{\alpha_1, ..., \alpha_n\}$ is a group of automorphisms of a field E with fixed field F then $[E : F] = |G|$.

Proof: Assume that the order of G is strictly smaller than $[E : F]$ and choose linearly independent elements $e_1, ..., e_{n+1}$ of E over F. The linear system over E defined by the n equations,

$$(1) \qquad \sum_{i=1}^{n+1} \alpha_j(e_i)x_i = 0, \text{ where } j \text{ takes values from 1 to } n$$

has more unknowns than equations, therefore it has a non-trivial solution. Among all n-tuples that correspond to a non-trivial solution choose one with the smallest number m of non-zero coordinates and represent, possisble after reindexings, it as $(\lambda_1, ..., \lambda_m, 0, ..., 0)$. $\lambda_i \neq 0$ for each i by minimality of m, clearly $m > 1$ and assume without loss of generality that $\lambda_m = 1$. Also, not all λ_i belong to F since otherwise a relation of linear dependence is obtained among $e_1, ..., e_{n+1}$ and therefore it is possible to assume that $\lambda_1 \notin F$. Choose a permutation π in G that does not fix λ_1 and plug in $x_1 = \lambda_1, ..., x_m = \lambda_m$ in (1) and use that G is a group to obtain,

$$(2) \qquad \sum_{i=1}^{n+1} \alpha_j(e_i)\pi(\lambda_i) = 0, \text{ where } j \text{ takes values from 1 to } n.$$

Now, again, plug in $\lambda_1, ..., \lambda_n$ in (1) to get $(1')$ and substract $(1')$ from (2) to see that $(\pi(\lambda_1) - \lambda_1, ..., \pi(\lambda_{m-1}) - \lambda_{m-1}, 0, ..., 0)$ is a solution to the linear system in consideration, contradiction. For the converse see Proposition 4.2.2.

Corollary 4.2.1 A field extension E/F is Galois iff $|\text{Gal}(E/F)| = [E : F]$.

Proof: By definition if E/F is Galois then $\mathcal{I}(\text{Gal}(E/F)) = F$, hence theorem 4.2.1 implies that $|\text{Gal}(E/F)| = [E : F]$. Conversely, if the condition is not satisfied $\mathcal{I}(\text{Gal}(E/F)) = F$ then by the tower law we get (theorem

1.1.1) $[E : F] > [E : \mathcal{I}(\mathrm{Gal}(E/F))]$. On the contrary by Proposition 4.2.3 we get $[E : \mathcal{I}(\mathrm{Gal}(E/F))] = \mathrm{Gal}(E/F)$, contradiction.

4.3 Normal and separable extensions

Definition 4.3.1 A finite field extension E/F is normal if every irreducible polynomial with coefficients in L which has a root in E splits in L.

Definition 4.3.2 A polynomial over a field F is called seperable if its irreducible factors do not have repeated roots. An algebraic extension field E of F is called separable if each element in E is a root of a separable polynomial over F.

Theorem 4.3.1 Let E/F be a field extension. Then the following are equivalent,

(α) E/F is a Galois extension,

(β) The extension E/F is normal and separable,

(γ) E is the splitting field of a separable polynomial $p(x)$ over F.

Proof: (α) $\Rightarrow$ (β) Let $\rho \in E$ be a root of an irreducible polynomial p over F and set $\mathcal{A} = \prod_{\rho \in P}(x - \rho)$, where $P = \{\alpha(\rho) : \alpha \in \mathrm{Gal}(E/F)\}$. The coefficients of $\mathcal{A}$ are left fixed by the automorphisms of $\mathrm{Gal}(E/F)$, therefore they are elements in $F = \mathcal{I}(\mathrm{Gal}(E/F))$. As p is irreducible and ρ a common root of p and $\mathcal{A}$ it follows that $p|\mathcal{A}$ and so p splits over E and is separable over F.

(β) $\Rightarrow$ (γ) Let $e_1, ..., e_n$ be a basis for E as a vector space over F and so $E = F(e_1, ..., e_n)$. Let p_i be the minimal polynomial of e_i over F. Each p_i splits over E as E/F is a normal extension and does not have multiple roots as E/F is separable. Therefore the polynomial $p = p_1 \cdots p_n$ is separable over F and as it splits over E its splitting field over F is E.

(γ) $\Rightarrow$ (α) For field extensions (E, F) satisfying (γ) and of degree one the extension E/F is Galois. Assume that for all field extensions of degree less than n the statement (γ) implies (α).

Let E/F be a field extension of degree n and E the splitting field of the separable polynomial p over F. If p splits over F then E/F is Galois, so assume that p has an irreducible factor q over F of degree $m > 1$. As q is separable it has m distinct roots $r_1, ..., r_m$. By Theorem 4.1.2 there are automorphisms $\alpha_1, ..., \alpha_m$ of $G = \mathrm{Gal}(E/F)$ such that $\alpha_i(r_1) = r_i$. Let k

be the number of distinct cosets of $H = \mathrm{Gal}(E/F(r_1))$ in G then $m \leq k$, since otherwise $\alpha_i H = \alpha_j H$ holds for distinct i and j and so ${\alpha_i}^{-1}\alpha_j \in H$ which in turns implies that $\alpha_i(r_1) = \alpha_j(r_1)$, contradiction. Now, Lagrange's Theorem gives, $|G| = k|H| \geq m|H|$.

On the other hand, the tower law implies that $[E : F(r_1)] < n$ and as p is separable over $F(r_1)$ it follows by induction that $E/F(r_1)$ is Galois and so Corollary 4.2.1 implies that $|\mathrm{Gal}(E/F(r_1)| = [E : F(r_1)]$. As, $m = [F(r_1) : F]$ finally we get that $|\mathrm{Gal}(E/F)| \geq [E : F(r_1)][F(r_1) : F] = [E : F]$ and as $|\mathrm{Gal}(E/F)| \leq [E : F]$ holds by Proposition 4.2.2 we get by Corollary 4.2.1 that E/F is Galois.

4.4 The fundamental theorem of Galois Theory

For a finite field extension E/F define two families of sets,

$$\mathcal{F} \doteq \mathcal{F}(E, F) = \{L : F \subseteq L \subseteq E \text{ and } L \text{ is a field}\}$$

$$\mathcal{G} \doteq \mathcal{G}(E, F) = \{H : H \text{ is a subgroup of } \mathrm{Gal}(E/F)\}$$

and two maps,

$$\begin{array}{rcl} \Phi : \ \mathcal{F} & \to & \mathcal{G} \\ L & \mapsto & \mathrm{Gal}(E/L) \end{array} \qquad \begin{array}{rcl} \Psi : \ \mathcal{G} & \to & \mathcal{F} \\ H & \mapsto & \mathcal{I}(H) \end{array}$$

It follows, directly, from the definitions of the Galois group $\mathrm{Gal}(\cdot/\cdot)$ and of the fixed field $\mathcal{I}(\cdot)$ that the maps Φ and Ψ are inclusion-reversing.

Proposition 4.4.1 Define the following subsets of $\mathcal{F}(E, F)$ and $\mathcal{G}(E, F)$,

$$\mathcal{F}' = \{L : L = \mathcal{I}(H) \text{ where } H \in \mathcal{G}(E, F)\}$$

$$\mathcal{G}' = \{H : H = \mathrm{Gal}(E/L) \text{ and } L \in \mathcal{F}(E, F)\}.$$

Let $\Phi' : \mathcal{F}' \to \mathcal{G}'$ be given by $L \mapsto \mathrm{Gal}(E/L)$ and $\Psi' : \mathcal{G}' \to \mathcal{F}'$ by $H \mapsto \mathcal{I}(H)$.

Then, Φ' and Ψ' are inclusion-reversing maps and mutual inverses.

Proof: That Φ and Ψ are inclusion reserving maps is clear. Suppose that $L \in \mathcal{F}'$ then $L = \mathcal{I}(H)$ for some $H \in \mathcal{G}$ and consider

$$\mathcal{I}(H) = L \ \xrightarrow{\Phi'} \mathrm{Gal}(E/L) \ \xrightarrow{\Psi'} \ \mathcal{I}(\mathrm{Gal}(E/L)$$

If the identity $L = \mathcal{I}(\mathrm{Gal}(E/L)$ holds then Φ' is clearly injective, surjective and $\Psi' \circ \Phi' = \mathrm{Id}_{\mathcal{F}'}$. Hence, it would follow that Φ' and Ψ' are mutual inverses.

($\subseteq$) $\forall\ l \in L : \alpha(l) = l$ holds for all $\alpha \in \mathrm{Gal}(E/L)$.

($\supseteq$) Every automorphism α in H leaves L invariant hence $\alpha \in \mathrm{Gal}(E/L)$, so $H \subseteq \mathrm{Gal}(E/L)$ and as Ψ is inclusion-reversing the inclusion follows.

Theorem 4.4.1 If the field extension E/F is Galois, then $\mathcal{F} = \mathcal{F}'$, $\mathcal{G} = \mathcal{G}'$ and the maps Φ and Ψ are mutual inverses.

Proof: If H is an element of $\mathcal{G}$ then it is a subgroup of $\mathrm{Gal}(E/L)$ hence $H = \mathrm{Gal}(E/\mathcal{I}(H))$ by Theorem 4.2.1, so $\mathcal{G} = \mathcal{G}'$. Let $L \in \mathcal{F}$ then by Theorem 4.3.1 E is the splitting field of a separable polynomial p over F. Clearly, then E is the splitting field of (the separable) p over L and so, again by Theorem 4.3.1, E/L is Galois and hence $L = \mathcal{I}(\mathrm{Gal}(E/L))$. That the maps Φ and Ψ are mutual inverses follows by Proposition 4.4.1.

Theorem 4.4.2, The fundamental theorem of Galois theory

Suppose that E is the splitting field of a separable polynomial p over F.

(α) There is a one-to-one inclusion-reversing correspondence between the set of intermediate fields of the field extension E/F and subgroups of the Galois group $\mathrm{Gal}(E/F)$.

(β) $N = \mathcal{I}(H)$ is a normal extension of F if and only if $H = \mathrm{Gal}(E/N)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. In this case there is an isomorphism $\mathrm{Gal}(N/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/N)$

(γ) For any $L \in \mathcal{F}(E, F)$ the degree of the E/L is equal to the order of $\mathrm{Gal}(E/L)$ and the degree of the extension L/F is equal to the index of $\mathrm{Gal}(E/L)$ in $\mathrm{Gal}(E/F)$.

Proof : (α) This is a consequence of Proposition 4.4.1 and Theorem 4.4.1.

(β) As N is normal and separable extension of F by Theorem 4.3.1 it is the splitting field of a polynomial f over F and so $N = F(r_1, ..., r_m)$, where $r_1, ..., r_m$ are the roots of f. Let α be an automorphism in $\mathrm{Gal}(E/F)$, then a root r_i is mapped under α to another root of f and as no root is the image under α of two distinct roots it follows that $\alpha(N) = N$. Hence, it is possible to define a map $\phi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(N/F)$ by sending $\alpha \in \mathrm{Gal}(E/F)$ to

$\tilde{\alpha} : N \to N$ where $\tilde{\alpha}$ satisfies $\tilde{\alpha}(x) = \alpha(x)$ for $x \in N$. It is straightforward to check that ϕ is a group homomorphism whose kernel is $\mathrm{Gal}(E/N)$. Hence, $\mathrm{Gal}(E/N)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. The surjectivity of ϕ, which follows by Theorem 4.1.2, shows that $\mathrm{Gal}(N/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/N)$.

Now, let H be a normal subgroup of G. Let $r \in \mathcal{I}(H)$ and let g be an irreducible polynomial over F of which r is a root and r' another root of g. Since, E/F is normal g splits over E and so Theorem 4.1.2 implies that there exists $\alpha \in \mathrm{Gal}(E/F)$ such that $\alpha(r) = r'$. Now, for any $\nu \in H$ the normality of H gives, $\nu(r') = \nu(\alpha(r)) = \alpha\alpha^{-1}(\nu(\alpha(r))) = \alpha(r) = r'$. So, $r' \in \mathcal{I}(H)$ and hence g splits over N.

(γ) We have already seen, in the proof of Theorem 4.4.1, that the field extension E/L is Galois for every $L \in \mathcal{F}(E, F)$. Hence, $|\mathrm{Gal}(E/L)| = [E : L]$ by Corollary 4.2.1. The second statement follows by the tower law.

A Appendix

A.1 The fundamental theorem of symmetric polynomials

The elementary symmetric polynomials $\sigma_1, ..., \sigma_n$ in the variables $x_1, ..., x_n$ are defined as follows:

$$\sigma_1 = x_1 + ... + x_n$$

$$\sigma_2 = \sum_{i<j} x_i x_j$$

$$\sigma_3 = \sum_{i<j<k} x_i x_j x_k$$

$$...$$

$$\sigma_n = x_1 \cdots x_n$$

Fact 5.1 Let R be a ring(commutative, with identity). If $p(x_1, ..., x_n)$ is a polynomial in the ring $R[x_1, ..., x_n]$ which reamains unaltered under any permutation of the roots then p is a polynomial in $F[\sigma_1, ..., \sigma_n]$.

A.2 The group structure of $U(\mathbb{Z}/(p))$

Fact 5.2 The multiplicative group of the field $\mathbb{Z}/(p)$ that is the the group $(\mathbb{Z}/(p) \setminus \{\mathbf{0}\}, \cdot)$ it is generated by a single element. In fact there are $\phi(p-1)$ such generators, where ϕ is the Euler ϕ function.

References

[1] Abel, N. H., Ouevres complétes de Niels Henrik Abel, Vol. 1, Grondahl, Christiania, 1881

[2] Artin E., Galois Theory, Dover Publications 1998

[3] Edwards H. M., Galois Theory, Springer-Verlag 1984

[4] Galois, É., Oeuvres Mathématiques d'Évariste Galois, Gauthier-Villars, Paris, 1897

[5] Kiernan B. M., The development of Galois theory from Lagrange to Artin, Archive for History of Exact Science 8, 1971, 40-154

[6] Lagrange, J.L, Réflexions sur la résolution algébrique des équations, Ouevres de Lagrange, vol.3 Gauthier-Villars, Paris, 1869

[7] Morandi P., Field and Galois Theory, Springer-Verlag 1996

[8] Tignol J-P, Galois' Theory of Algebraic Equations, World Scientific 2001

[9] WIKI – ΠΑΙΔΕΙΑ, For various definitions and bi(bli)ographical data of ... Emil Artin, Évariste Galois, Niels Henrik Abel, Carl Friedrich Gauss, Alexandre-Théophile Vandermonde, Joseph-Louis Lagrange, ..., $\Pi\upsilon\theta\alpha\gamma\acute{o}\rho\alpha\varsigma$ *o* $\Sigma\grave{a}\mu\iota o\varsigma$, ...