Galois Theory and Solvable Equations of Prime Degree*

Anirban Ghatak[1] AND Anshoo Tandon[2]

[1]Department of ECE, IISc. Bangalore

[2]Alumnus, Department of ECE, IISc. Bangalore; presently at Broadcom, Bangalore

E-mail: [1]aghatak@ece.iisc.ernet.in and [2]anshoo.tandon@gmail.com

*The authors gratefully acknowledge Prof. D. P. Patil, Department of Mathematics/ Computer Science and Automation, for encouraging us to write this article; providing many innovative proofs of classical results in modern language and historical comments.

Abstract | In this article we review classical and modern Galois theory with historical evolution and prove a criterion of Galois for solvability of an irreducible separable polynomial of prime degree over an arbitrary field k and give many illustrative examples.

Introduction

This is an (expository) article on Galois theory which is inspired and influenced by several lectures[1] of Prof. D. P. Patil and a short course of lectures[2] by Prof. U. Storch.

The basic idea of Galois was to associate with any polynomial (over a field) a group of permutations of its roots (zeroes), the so-called *Galois group*. This group consists of all the permutations which preserves the relations among the roots and hence it provides a new tool to measure to what extent which roots of the given equation are permuted. Galois' brilliant insight was that this group provides an effective measure of the difficulty of understanding the roots of an equation and he derived the conditions for an equation to be solvable by radicals. In particular, the solvability of the equation by radicals can be translated in terms of the Galois group which leads to the notion of solvable groups.

In order to make the article self-contained, in Section 1 we review classical and modern Galois theory with historical evolution in many footnotes and give many illustrative examples. In Subsection 1.C we prove Jordan's Lemma (see 1.C.1) which played a very crucial role in the development of modern Galois theory and justify this by its use. We also give the formulation of the Galois' Great Theorem (see 1.D.2) in arbitrary characteristic and its complete proof in Subsection 1.D. As an application we prove a Theorem (see 1.D.8) of Hölder on solvability by real radicals and deduce its consequences. In Section 2 we prove the solvability of the affine group of an affine line over $\mathbb{F}_p$ and give

[1]Starting with a special course under the title "Arithmetic, Algebra and Geometry – With a view towards applications" which was initiated by Prof. D. P. Patil in the Institute during 2005-06. This course stimulated many of us into active learning, boosted our confidence and introduced us to the excitement of doing mathematics. Moreover, we learnt many important mathematical concepts and examples from his short course on "Galois Theory and Class Numbers" delivered in the IMI Workshop on Number Theory and Cryptography during Jan-Feb 2006.

[2]A short course on "Galois Theory" by Prof. U. Storch, Ruhr Universität, Bochum, Germany during his visit in December 2009. We were stimulated as much by the sheer brilliance of his pedagogy as his very friendly and charming style while he gave us an exposition of the classical results with lots of examples.

a characterisation of transitive solvable subgroups of the permutation group $\mathfrak{S}_p$, where p is a prime number. With these fertile ideas developed in Section 1 and Section 2, in Section 3 we prove the classical theorem of Galois on the solvability of equations of prime degree over an arbitrary field k.

§ 1 Review of Galois Theory

In this section we shall review classical and modern Galois theory with historical evolution and provide many examples to illustrate concepts.

1.A Field Extensions

We begin with basic notations and definitions of field extensions which will be used in later subsections and sections.

For a field extension $K|k$, let $\mathrm{Gal}(K|k) := \mathrm{Aut}_{k\text{-alg}}\, K$ denote the group of k-algebra automorphisms $\sigma : K \to K$ of the field K. This group is called the Galois group[3] (or symmetry group) of $K|k$; its elements are the field automorphisms of K which fix the elements of k. For an arbitrary subgroup $H \subseteq \mathrm{Gal}(K|k)$, the subfield $\mathrm{Fix}_H K := \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ of K which contains k is called the fixed or invariant field of H in K. The classical Galois theory deals with the interplay between the subgroups of $\mathrm{Gal}(K|k)$ and intermediary subfields of $K|k$. Throughout this article we consider only *finite* field extensions $K|k$, i. e. the field K is a finite dimensional vector space over the subfield k; the k-vector space dimension $\mathrm{Dim}_k K$ of K, which is also called the degree of the field extension, is usually denoted by $[K : k]$. In this case, every element $x \in K$ is algebraic over k, i. e. there exists a non-zero polynomial f in the polynomial algebra $k[X]$ over k with $f(x) = 0$. More generally, a field extension $K|k$ is algebraic if every element of K is algebraic over k. The minimal polynomial $\mu_{x,k} \in k[X]$ of x over k is the monic polynomial of least degree in $k[X]$ for which $\mu_{x,k}(x) = 0$. Equivalently, $\mu_{x,k}$ is the monic generator of the kernel of the substitution (k-algebra) homomorphism $\varepsilon_x : k[X] \to K$, $f(X) \mapsto f(x)$. In particular, since K is a field, $\mu_{x,k}$ is irreducible in $k[X]$ and the smallest subring $k[x]$ is equal to the smallest subfield $k(x)$ containing k and x, i. e. $k[x] = k(x)$ and $[k(x) : k] = \deg \mu_{x,k}$.

Two elements $x, y \in K$ of a field extension $K \supseteq k$ are called conjugates over k, if they are algebraic over k and have the same minimal polynomial, i. e. $\mu_{x,k} = \mu_{y,k}$. If the degree of the minimal polynomial $\deg \mu_{x,k} = n$, then the number of conjugates of x over k is at most n. Moreover, if x and y are conjugates over k, then the fields $k(x)$ and $k(y)$ are isomorphic over k. Therefore, *if $g \in k[X]$ is an irreducible polynomial, then there*

[3] This definition of the Galois group is very different from the one given by Évariste Galois (1811-1832). In fact, he defined the Galois group of splitting fields and it consisted of certain permutations of the roots which respect the algebraic structure of the roots, i. e. which come from the automorphisms of the splitting field (see Footnote 4 and Example 1.C.12). Isomorphisms of fields were first defined by Richard Dedekind (1831-1916) in 1877. By 1894 Dedekind was also aware of the relevance of automorphisms to Galois theory. Dedekind's influence can be seen in the three volumes of *Lehrbuch der Algebra* by his student Heinrich Weber (1842-1913) which appeared in 1884; starting with the Galois definition of the Galois group it gives a careful account of Galois theory leading to automorphisms of splitting fields.

exists – upto k-algebra isomorphism – at most one simple extension $k(x)|k$ such that x is a zero of g. More generally:

1.A.1 Lemma *Let $K|k$ and $K'|k$ be two field extensions of k and let $x \in K$, $x' \in K$ be algebraic over k. Then $\mu_{x,k} = \mu_{x',k}$ if and only if there exists a k-algebra isomorphism $k(x) \xrightarrow{\sim} k(x')$.*

1.A.2 Canonical Operation of the Galois group Let $K|k$ be an algebraic field extension with Galois group $\mathrm{G} := \mathrm{Gal}(K|k)$. Then the group G operates canonically on the field K by (automorphisms of k-algebras): $\mathrm{G} \times K \to K$, $(\sigma, x) \mapsto \sigma(x)$. The orbit $\mathrm{G}x$ of an element $x \in K$ under this operation[4] is the set of zeroes of the minimal polynomial $\mu_{x,k}$ in K. By Lemma 1.A.1 this set is precisely the set of conjugates of x over k in K. In particular, $\#\mathrm{G}x \leq [k(x) : k] = \deg \mu_{x,k}$. The fixed point set $\mathrm{Fix}_{\mathrm{G}} K$ is a subfield of K containing k and is called the fixed field of $K|k$ under the operation of G. In particular, $[K : \mathrm{Fix}_{\mathrm{G}} K]$ divides $[K : k]$. For basic results on group action, see [6, Section 1].

1.A.3 Algebraic closure and embeddings (see also Footnote 34) Let $K|k$ be a field extension. We say that K is an algebraic closure of K if $K|k$ is an algebraic extension of k and if K is algebraically closed field, i. e. if every non-constant polynomial in $K[X]$ has at least one root in K, or equivalently, it factors completely into linear polynomials in $K[X]$. The following fundamental theorem guarantees the existence and the essential unicity of an algebraic closure of a given field k: *Let k be a field. Then there exists an algebraic closure of k and any two algebraic closures of k are isomorphic over k.* Moreover, the second half of this theorem is included in the following stronger result: *Let Ω be an algebraically closed field and let $K|k$ be an algebraic extension of a field k. If $\sigma_0 : k \to \Omega$ is a homomorphism of fields, then σ_0 can be extended to a homomorphism of fields $K \to \Omega$.*

With these results, for every field k we fix *the* algebraic closure $\bar{k}$ of k. Then every algebraic extension $K|k$ can be embedded in $\bar{k}$ as a subfield. Therefore for any two algebraic extensions $K|k$ and $K'|k$ of a field k, we can always consider their compositum in the algebraic closure $\bar{k}$ of k. See also Footnote 31.

1.B Galois Extensions

In this subsection we shall review classical Galois theory from the modern point of view[5] which will lead to the Fundamental Theorem of Galois Theory 1.B.11. This theorem allows us to translate many questions about fields into finite groups.

[4] For a field extension $K|k$, $\sigma \in \mathrm{Gal}(K|k)$ and a polynomial $h \in k[X]$, it follows that $\sigma(h(x)) = h(\sigma(x))$ for every $x \in K$. In particular, if $x \in K$ is a zero of h in K, then $\sigma(x)$ is also a zero of h in K.

[5] The first steps towards the new subjects such as the theory of groups and various algebraic structures, in particular, field theory, were the works of Leopold Kronecker (1823-1891) and Dedekind. Moreover, linear algebra was brought to the theory of fields as the field extension is regarded as a vector space over the smaller field. These ideas became more popular in the first decades of the twentieth century. Evolution was made by Emil Artin (1898-1962) by his definition of Galois group ((ii) of Theorem 1.B.5), which was given in 1920's as the starting point of Galois theory. The first exposition of this appeared in the famous treatise of Bartel Leendert Van der Waerden (1903-1996) – "Moderne Algebra". Artin published his own account of Galois theory in 1938 and 1942 (see [2]). The latter was enormously influential with more emphasis on fields and groups while polynomials and equations play a secondary role and are used as tools in the proofs. The main theorems do not involve polynomials in their statements and hence the Fundamental Theorem of Galois Theory can be proved without ever mentioning polynomials.

Let $K|k$ be a finite field extension, then from the well-known *Dedekind-Artin Lemma*[6] it follows that $\#\,\mathrm{Gal}(K|k) \leq [K:k]$. A finite field extension $K|k$ is called a Galois extension if the equality $\#\,\mathrm{Gal}(K|k) = [K:k]$ holds.

1.B.1 Example The Galois group of the field $\mathbb{C}$ of complex numbers over the field of real numbers $\mathbb{R}$ is $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$, where $\sigma : \mathbb{C} \to \mathbb{C}$ is the complex conjugation $z \mapsto \bar{z}$. Therefore the field extension $\mathbb{C}|\mathbb{R}$ is a Galois extension. The field extension $\mathbb{C}|\mathbb{Q}$ is infinite and its Galois group $\mathrm{Gal}(\mathbb{C}|\mathbb{Q})$ is also infinite! For a field k of characteristic $p > 0$, the Galois group $\mathrm{Gal}(k(X)|k(X^p)) = \{\mathrm{id}_{k(X)}\}$, where $k(X)$ (respectively, $k(X^p)$) denotes the rational function field in indeterminate X (respectively, X^p). The degree of $k(X)|k(X^p)$ is p and hence the field extension $k(X)|k(X^p)$ is not a Galois extension.

1.B.2 Example (Simple Galois extensions) For a simple (algebraic) field extension $k(x)$ of a field k, the natural map $\mathrm{Gal}(k(x)|k) \to \mathrm{V}_{k(x)}(\mu_{x,k})$, $\sigma \mapsto \sigma(x)$ is injective, where $\mathrm{V}_{k(x)}(\mu_{x,k}) = \{x = x_1, x_2, \ldots, x_n\}$ denotes the set of zeroes of $\mu_{x,k}$ in $k(x)$. In particular, $\#\,\mathrm{Gal}(k(x)|k) \leq \deg \mu_{x,k} = [k(x):k]$. Therefore equality holds, i. e. $k(x)|k$ is Galois extension if and only if $\mu_{x,k} = (X - x_1)\cdots(X - x_n) \in k(x)[X]$ splits into simple linear factors over $k(x)$; equivalently, $\mu_{x,k}$ is *separable*[7] over k. Moreover, in this case, $\mathrm{Gal}(k(x)|k) = \{\sigma_{x_1}, \ldots, \sigma_{x_n}\}$, where $\sigma_{x_i} : k(x) \to k(x)$ are the substitution automorphisms $x = x_1 \mapsto x_i$, $i = 1, \ldots, n$.

1.B.3 Example (Cyclotomic extensions) A field extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}$, where $\zeta_n = e^{2\pi \mathrm{i}/n}$, $n \in \mathbb{N}^*$, is called a cyclotomic extension[8]. A study of cyclotomic extensions involves the study of cyclotomic polynomials and Gauss' theory of periods. These results are applied to determine which regular polygons are *constructible by straightedge and compass*[9]. More generally, one can also consider *n-th roots of unity*[10] over an arbitrary field k of characteristic

---

[6] A character of a monoid M in a field K is a monoid homomorphism χ from M into the multiplicative group $K^\times (:= K \setminus \{0\})$ of the field K. *Every set $\{\chi_1, \ldots, \chi_n\}$ of distinct characters of a monoid M in a field K is linearly independent over K. In particular, every set $\{\sigma_1, \ldots, \sigma_n\}$ of distinct automorphisms of a field K is linearly independent over K.*

[7] Recall that a polynomial f is separable if $f \neq 0$ and $\mathrm{GCD}(f, f') = 1$, where f' is the derivative $\frac{\mathrm{d}}{\mathrm{dX}}(f)$ of f, or equivalently, if the discriminant $\mathrm{Disc}(f)$ of f is $\neq 0$. Recall that if $x_1, \ldots, x_n$ are all zeroes of f, then the discriminant $\mathrm{Disc}(f)$ is defined by the equation $\mathrm{Disc}(f) = \prod_{1 \leq i < j \leq n}(x_i - x_j)^2$ which is a symmetric polynomial in the zeroes $x_1, \ldots, x_n$ of f and hence is a polynomial in the elementary symmetric functions (see Footnote 22) $\mathrm{S}_1(x_1, \ldots, x_n), \ldots, \mathrm{S}_n(x_1, \ldots, x_n)$, i. e. the coefficients of f and hence $\mathrm{Disc}(f) \in k$. For $n = 3$, the discriminant is implicit in Cardano's formulae (see Footnote 34). By 1770 Joseph-Louis Lagrange (1736-1813) and Alexandre-Théophile Vandermonde (1735-1796) knew properties of $\mathrm{Disc}(f)$ and its square root $\Delta_f := \sqrt{\mathrm{Disc}(f)} = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ for small values of n. This Δ_f is also known as the Vandermonde determinant of $x_1, \ldots, x_n$ and is denoted by $\mathrm{V}(x_1, \ldots, x_n)$. The general form of the discriminant was defined independently by Augustin-Louis Cauchy (1789-1857) in 1815 and by Johann Carl Friedrich Gauss (1777-1855) in 1816.

[8] Both Lagrange and Vandermonde made significant use of roots of unity. The first systematic study of cyclotomic extensions is due to Gauss. Most of Gauss' results appear in *Disquisitiones Arithmeticae* published in 1801. Gauss studies the extension $\mathbb{Q}(\zeta_p)|\mathbb{Q}$, where p is a prime number. He constructs primitive elements for intermediary subfields, essentially describes Galois correspondence and uses these results to show that the equation $x^p - 1 = 0$ is solvable by radicals (over $\mathbb{Q}$).

[9] The idea of geometric constructions using straightedge and compass goes back to the ancient Greeks. Some of the most famous problems in Greek geometry are *duplication of the cube, trisection of angles* and *squaring the circle*. In 1837 Pierre Laurent Wantzel (1814-1848) showed that the duplication of the cube and the trisection of the angle cannot be done by straightedge and compass by using the irreducibility of certain cubic polynomials. More generally: *Every constructible number is algebraic over $\mathbb{Q}$ and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2, where constructible numbers are complex numbers which are obtained as the points of intersections of lines and circles by using a finite sequence of straightedge and compass constructions starting with the numbers 0 and 1.* The set $\mathfrak{C}$ of constructible numbers form a subfield of $\mathbb{C}$ and is closed under the operation of square roots, i. e. if $x \in \mathfrak{C}$, then $\sqrt{x} \in \mathfrak{C}$. In 1796 Gauss proved: *The regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2, equivalently, $n = 2^m p_1 \cdots p_r$, where $p_1, \ldots, p_r$ are pairwise distinct Fermat-primes.* – The natural number $\mathrm{F}_m = 2^{2^m} + 1$ is called the n-th Fermat-number, named after Pierre de Fermat (1601-1665) who thought they might all be primes. Fermat-numbers which are prime are called Fermat-primes. The only known Fermat-primes are $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3, \mathrm{F}_4$; $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ divides $5^4 \cdot 2^{28} + 2^{32}$ and $5^4 \cdot 2^{28} - 1$ and therefore divides the difference $2^{32} + 1 = \mathrm{F}_5$. Further, the Fermat-numbers F_t, $5 \leq t \leq 36$ are not primes. It is conjectured that there are only finitely many Fermat-primes, but it is still open.

[10] Let k be a field. The elements $\mathbf{W}(k) := \{x \in k^\times \mid \mathrm{ord}\, x < \infty\}$ of the multiplicative group $k^\times$ of k of finite order are called the roots of unity in k. For $n \in \mathbb{N}$, the elements of the subset $\mathbf{W}_n(k) := \{\zeta \in k^\times \mid \zeta^n = 1\} \subseteq \mathbf{W}(k)$ are called the n-th roots

coprime to n. *The splitting field of the polynomial* X^n-1 *over* k *is* $k(\zeta_n)$ *and* $k(\zeta_n)|k$ *is a Galois extension with Galois group* $\mathrm{Gal}(k(\zeta_n)|k) \xrightarrow{\sim} (\mathbb{Z}_n)^\times$ (= the unit group of the ring $\mathbb{Z}_n$ of integers modulo n.)

1.B.4 Example (Finite fields[11]) Let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ be finite fields with q and q^n elements, respectively. Then $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$ and the Frobenius automorphism $\mathrm{f}_q:\mathbb{F}_{q^n}\to\mathbb{F}_{q^n}$, $x\mapsto x^q$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ generates the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$. In particular, $\mathbb{F}_{q^n}|\mathbb{F}_q$ is a Galois extension of degree n with cyclic Galois group.

1.B.5 Theorem (Artin) *For a finite field extension* $K|k$ *the following statements are equivalent*:

(i) $K|k$ *is Galois extension.*

(ii) $\mathrm{Fix}_{\mathrm{Gal}(K|k)}K=k$.

(iii) K *is the splitting field of a separable polynomial* $f\in k[X]$.

1.B.6 Trace and Norm Let $K|k$ be a finite Galois extension with Galois group $\mathrm{G}:=\mathrm{Gal}(K|k)$. Then for every $x\in K$, we have

(1) *The characteristic polynomial* $\chi_{x,k}=\prod_{\sigma\in\mathrm{G}}(X-\sigma(x))$. *In particular, the trace*[12] *of* x *over* k *is* $\mathrm{tr}_k^K(x):=\mathrm{tr}(\lambda_x)=\sum_{\sigma\in\mathrm{G}}\sigma(x)$ *and the norm of* x *over* k *is* $\mathrm{N}_k^K(x):=\mathrm{Det}(\lambda_x)=\prod_{\sigma\in\mathrm{G}}\sigma(x)$, where $\lambda_x:K\to K$ denotes the multiplication by x which is clearly a k-linear map on the k-vector space K.

(2) *The minimal polynomial* $\mu_{x,k}$ *of* x *over* k *is* $\mu_{x,k}=\prod_{y\in\mathrm{G}x}(X-y)$. *Further,* $\chi_{x,k}=\left(\mu_{x,k}\right)^{\#\mathrm{G}_x}$. *In particular,* $\deg\mu_{x,k}=[k(x):k]=\#\mathrm{G}x=[\mathrm{G}:\mathrm{G}_x]$.

1.B.7 Resolvents Let $K|k$ be a finite field extension with Galois group $\mathrm{G}:=\mathrm{Gal}(K|k)$. An element $y\in K$ is called a Galois resolvent[13] of $K|k$ if $K=k(y)$ and $K|k$ is Galois extension. Equivalently (see Example 1.B.2), the minimal polynomial $\mu_{y,k}\in k[X]$ of y over k splits completely into simple linear factors $\mu_{y,k}=(X-y_1)\cdots(X-y_n)\in K[X]$

---

of unity in k. Clearly $\mathbf{W}(k)$ and $\mathbf{W}_n(k)$ are subgroups of $k^\times$ and $\mathbf{W}(k)=\bigcup_{n\in\mathbb{N}}\mathbf{W}_n(k)$. Further, $\mathbf{W}_n(k)$ is a finite and hence cyclic subgroup of $k^\times$; its order $\#\mathbf{W}_n(k)$ divides n. An element $\zeta\in\mathbf{W}_n(k)$ of order n is called a primitive n-th root of unity. If $\mathrm{Char}k=p>0$, then $\mathbf{W}_{np}(k)=\mathbf{W}_n(k)$. Further, if k is algebraically closed, then for every $n\in\mathbb{N}$ coprime to p, $\#\mathbf{W}_n(k)=n$ and hence k contains a primitive n-th root of unity ζ and any such primitive n-th root of unity is a generator of $\mathbf{W}_n(k)$. If $\mathrm{Char}k=p>0$, for arbitrary $n\in\mathbb{N}$, $\#\mathbf{W}_n(k)=n\cdot p^{-v_p(n)}$. Moreover, it follows immediately from Chinese Remainder Theorem that $\mathbf{W}_n(k)\cong\prod_{q\neq\mathrm{Char}k}\mathbf{W}_{q^{v_q(n)}}(k)$.

The polynomial X^n-1 over a field k of characteristic coprime to n is separable and its zeroes (in the algebraic closure $\bar{k}$) $\mathbf{W}_n(\bar{k})=\mathrm{V}(X^n-1)$ form a subgroup of $\bar{k}\setminus\{0\}$ and hence is cyclic of order n ; a generator ζ_n of this group is called a primitive n-th root of unity. Therefore $k(\zeta_n)$ is the splitting field of X^n-1 over k and $X^n-1=\prod_{\zeta\in\mathbf{W}_n}(X-\zeta)=\prod_{d|n}\Phi_d(X)$, where $\Phi_d(X)=\prod_{\substack{\zeta\in\mathbf{W}_n\\ \mathrm{ord}\,\zeta=d}}(X-\zeta^i)\in\mathbb{Z}[X]$ with $\deg\Phi_d=\varphi(d)$, where φ denotes the *Euler's totient function*, is the prime decomposition of X^n-1 in $\mathbb{Z}[X]$. The polynomial $\Phi_n(X)=\prod_{\substack{\zeta\in\mathbf{W}_n\\ \mathrm{ord}\,\zeta=n}}(X-\zeta^i)=\prod_{\substack{0\le i<n\\ \gcd(i,n)=1}}(X-\zeta_n^i)\in\mathbb{Z}[X]$ is called the n-th cyclotomic polynomial which is the minimal polynomial of ζ_n over $\mathbb{Q}$ and hence $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})=[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)=\#(\mathbb{Z}_n)^\times$. The first published proof that Φ_n is irreducible over $\mathbb{Q}$ appeared in 1854 and is due to Kronecker. Gauss proved this for $n=p$ prime by using *Gauss' lemma*.

[11] Galois was the first to consider finite fields as field extensions of their prime subfields, but he said nothing about their existence. He simply performed computations in them.

[12] One can also directly define the trace $\mathrm{tr}_k^K(x)$ and the norm $\mathrm{N}_k^K(x)$ of an element x in a Galois extension by these formulae without using the characteristic polynomial $\chi_{x,k}$ of $\lambda_x:K\to K$. Further, since these elements are invariant under all $\sigma\in\mathrm{Gal}(K|k)$, they belong to k. The k-linearity of the trace map $\mathrm{tr}_k^K:K\to k$ and the multiplicativity of the norm map $\mathrm{N}_k^K:K\to k$ follow directly from these formulae.

[13] This terminology (which is of course not due to Galois) stems from the observation that in order to solve the equation $\pi(x)=0$ it is sufficient to determine y, since the roots $x_1,\ldots,x_n$ of $\pi(x)=0$ are rational functions in y with coefficients in k. It is preferable to call the minimum polynomial $\mu_{y,k}$ the Galois resolvent (polynomial) rather than the element y. See also Footnote 36.

with $y = y_1, \ldots, y_n \in K$ and $n = [K : k]$. In particular, *an element $y \in K$ is a Galois resolvent of $K|k$ if and only if* G_y *at y is trivial,* i. e. $G_y = \{\mathrm{id}_K\}$.

1.B.8 Theorem (Primitive Element[14] Theorem) *Let $K|k$ be a finite Galois extension with Galois group* $G := \mathrm{Gal}(K|k)$. *Then K has a Galois resolvent over k,* i. e. *there exists an element $y \in K$ such that the isotropy group* G_y *at y is trivial.*

The proof is immediate from the observation[15] from Linear Algebra applied to the subspaces $V_\sigma = \{x \in K \mid \sigma(x) = x\}$, $\sigma \neq \mathrm{id}_K$ of the vector space K over k.

1.B.9 Example Let F be a field of characteristic $p > 0$, U, V be indeterminates over F and let $k := F(U,V)$ be the field of rational functions in U and V over F.
Let $f := (X^p - U)(X^p - V) \in k[X]$. Then the splitting field of f over k is $K := k(u,v)$, where $u^p = U$ and $v^p = V$. Further, $[K : k] = p^2$, $[k(y) : k] = p$ for every $y \in K \setminus k$, in particular, $K|k$ has no primitive element and it is not a Galois extension. Further, $\mathrm{Gal}(K|k) = \{\mathrm{id}\}$,
since $f = (X^p - U)(X^p - V) = (X - u)^p (X - v)^p$ in $K[X]$. Moreover, the intermediary subfields $k(u + \lambda v)$, $\lambda \in F$ are all distinct. In particular, if F is infinite, then $K|k$ has infinitely many intermediary subfields (see also Footnote 14). However, if $p = 3$ and if K' is the splitting field of $g := (X^2 - U)(X^3 - V)$ over k, then there exists a primitive element for $K'|k$, but $K'|k$ is not separable. In fact, $K' = k(u,v)$, where $u^2 = U$, $v^3 = V$ and $[K' : k] = [k(u,v) : k(v)] \cdot [k(v) : k] = 2 \cdot 3 = 6$, $\mathrm{Gal}(K'|k) = \{\mathrm{id}, \sigma\}$, where $\sigma(u) = -u$ and $\sigma(v) = v$. Moreover, the element $u + v$ is a primitive element for $K'|k$ with the minimal polynomial $(X - u - v)^3 (X + u - v)^3 = X^6 - 2VX^3 - U^3 + V^2 \in k[X]$.

1.B.10 Conjugate subfields Let $K|k$ be a field extension. Let $k \subseteq L \subseteq K$ be an intermediary subfield and let $\sigma \in \mathrm{Gal}(K|k)$. Then the image $\sigma(L)$ of L under σ is again an intermediary subfield of $K|k$ and is called a conjugate subfield of L in K.

Let $K|k$ be a Galois extension. It is clear that $L = \sigma(L)$ *if and only if* $\mathrm{Gal}(K|L) = \sigma\,\mathrm{Gal}(K|L)\sigma^{-1}$ *in the Galois group* $\mathrm{Gal}(K|k)$ or, equivalently, σ *belongs to the normaliser of the subgroup* $\mathrm{Gal}(K|L)$ *of* $\mathrm{Gal}(K|k)$. In particular, the number of intermediary subfields conjugate to L of $K|k$ is the index $[\mathrm{Gal}(K|k) : N]$, where N is the normaliser of $\mathrm{Gal}(K|L)$ in $\mathrm{Gal}(K|k)$. More precisely, the Galois group $\mathrm{Gal}(K|k)$ operates on the set of conjugate subfields of L and the isotropy group at L is the normaliser of $\mathrm{Gal}(K|L)$ in $\mathrm{Gal}(K|k)$. Therefore: *for an intermediary subfield $k \subseteq L \subseteq K$ of a Galois extension $K|k$, the following statements are equivalent*:

(i) $L = \sigma(L)$ *for every* $\sigma \in \mathrm{Gal}(K|k)$.
(ii) $\mathrm{Gal}(K|L)$ *is a normal subgroup of* $\mathrm{Gal}(K|k)$.
(iii) $L|k$ *is a Galois extension.*
(iv) $L|k$ *is a normal extension* (see Footnote 18).

1.B.11 Theorem (Fundamental Theorem of Galois Theory - Galois correspondence) *Let $K|k$ be a finite Galois extension. Then for every intermediary subfield L of $K|k$, the field extension $K|L$ is again a Galois extension and the maps*

[14] An element y is called a primitive element of the field extension $K|k$ if $K = k(y)$. Galois resolvents of the Galois extension $K|k$ are primitive elements of $K|k$. More generally, all finite separable extensions have primitive elements, but not conversely. A characterisation: *A finite field extension $K|k$ has a primitive element if and only if there are only finitely many intermediary subfields* was proved by Ernst Steinitz (1871-1928).

[15] If $V_1, \ldots V_m$ are proper subspaces of a finite dimensional vector space V over a field k with $\#k \geq m$, then $V_1 \cup \cdots \cup V_m \subsetneq V$. Proof by induction on m. Choose $v \in V_m \setminus (V_1 \cup \cdots \cup V_{m-1})$ and $w \in V \setminus V_m$. Then consider the distinct vectors $av + w$, $a \in k$.

$L \mapsto \mathrm{Gal}(K|L)$ and $H \mapsto \mathrm{Fix}_H K$ are inclusion-reversing bijective maps of the set of intermediary subfields of $K|k$ and the set of subgroups of the Galois group $\mathrm{Gal}(K|k)$ which are inverses of each other, i. e. *$L = \mathrm{Fix}_{\mathrm{Gal}(K|L)} K$ and $\mathrm{Gal}(K|\mathrm{Fix}_H K) = H$. Moreover, under these bijections, the degrees of intermediary subfields over k correspond to the indices of corresponding subgroups in $\mathrm{Gal}(K|k)$,* i. e. *$[L:k] = [\mathrm{Gal}(K|k) : \mathrm{Gal}(K|L)]$ and $[\mathrm{Gal}(K|k) : H] = [\mathrm{Fix}_H K : k]$. Furthermore, an intermediary subfield L of $K|k$ is Galois over k if and only if the corresponding subgroup $\mathrm{Gal}(K|L)$ is normal in $\mathrm{Gal}(K|k)$ and in this case the restriction homomorphism $\mathrm{Gal}(K|k) \to \mathrm{Gal}(L|k)$ induces an isomorphism $\mathrm{Gal}(K|k)/\mathrm{Gal}(K|L) \xrightarrow{\sim} \mathrm{Gal}(L|k)$.*

1.B.12 Remark The Example 1.B.9 shows that the Galois correspondence can break down spectacularly for purely inseparable splitting fields.

1.B.13 Remark Gauss studied the extension $\mathbb{Q}(\zeta_p)|\mathbb{Q}$, where p is an odd prime and ζ_p is a primitive p-th root of unity and described the intermediate field by using *Gauss periods* and used these results to show that the pure equation $x^p - 1 = 0$ is solvable.

1.C Galois Group of a Polynomial

In this subsection we shall study the Galois groups of the splitting fields of polynomials with separable reduction. As suggested by the Fundamental Theorem of Galois Theory 1.B.11 we study the roots of polynomial equations by using the key notion of *group action* in group theory. We illustrate many classical concepts, results and examples using the modern language of group actions.

Let k be a field, $f \in k[X]$ and $f = a\pi_1^{\nu_1} \dots \pi_r^{\nu_r}$ be the prime factorisation of f in $k[X]$, where $a \in k^\times$, $\nu_1 \dots \nu_r > 0$ are positive natural numbers and $\pi_1, \dots, \pi_r \in k[X]$ are distinct prime factors of f in $k[X]$. Then the (simple) product $\mathrm{Red} f := \pi_1 \dots \pi_r$ is called the r e d u c t i o n of f. We assume that $\mathrm{Red} f$ is separable[16] over k. Then by a classical theorem of Kronecker[17], *there exists a finite field extension $K|k$ such that the polynomial f splits into linear factors over K*, i. e. *in $K[X]$ one has $f = (X - x_1)^{\nu_1} \cdots (X - x_n)^{\nu_n}$ with pairwise distinct $x_1, \dots, x_n \in K$* (since $\mathrm{Red} f$ is separable). The subfield $K = k(x_1, \dots, x_n)$ is generated over k by the set $\mathrm{V}(f) = \{x_1, \dots, x_n\}$ of all zeroes of f in the algebraic closure of k (see Footnote 34) and is called the (m i n i m a l) s p l i t t i n g f i e l d of f over k. It is a finite Galois extension and is uniquely determined [18] by f upto k-algebra isomorphism. The group $\mathrm{Gal}(K|k)$ of all k-automorphisms of K is called the

[16] Equivalently, all prime factors $\pi_1, \dots, \pi_r$ of f are separable over k, in this case we say that f has a s e p a r a b l e r e d u c t i o n.

[17] The construction of the splitting field of an arbitrary polynomial $f \in k[X]$ over an arbitrary field k is due to Kronecker. He was inspired by Galois' approach to the Galois group and drew ideas from Lagrange, Gauss and Galois to create a field extension $K|k$ in which f splits completely using a single quotient rather than using a sequence of quotients. Kronecker's construction of the splitting field contains a lot of information about the roots of the polynomial f and it leads directly to an algorithm for computation of the Galois group of f.

[18] For a proof of the uniqueness theorem on splitting fields of an arbitrary polynomial $f \in k[X]$, we restate the assertion of the Lemma 1.A.1 in a sightly more general form which will be used in the inductive step.

Lemma *Let $\tau : k \xrightarrow{\sim} k'$ be an isomorphism of two fields, $f \in k[X]$ and let $f' := \tau(f(x)) \in k'[X]$ be the corresponding polynomial in $k'[X]$ (obtained by applying τ to the coefficients of f). Further, let x (respectively, x') be a zero of f (respectively, f') in some field extension of k (respectively, k'). Then the isomorphism τ can be extended uniquely to an isomorphism $\rho : k(x) \to k'(x')$ such that $\rho(x) = x'$.*

Using the above lemma one can now prove the uniqueness theorem on the splitting fields, more precisely:

Uniqueness of splitting fields *Let $\tau : k \xrightarrow{\sim} k'$ be an isomorphism of fields, $f \in k[X]$ and let $f' := \tau(f(x)) \in k'[X]$ be the*

Galois group of the polynomial f or the equation $f(x)=0$ over k and is usually denoted by $\mathrm{G}_k(f)$. Note that $\mathrm{V}(f)=\mathrm{V}(\mathrm{Red}\,f)$, $\#\mathrm{V}(f)=\deg(\mathrm{Red}\,f)$ and $\mathrm{G}_k(f)=\mathrm{G}_k(\mathrm{Red}\,f)$. It is clear that $\#\mathrm{G}_k(f)=[K:k]\le\#\mathrm{V}(f)\le(\deg f)!$.

Since the image $\sigma(x)$ of any zero x of f under a k-algebra automorphism $\sigma\in\mathrm{G}_k(f)$ is again a zero of f (see Footnote 4), the canonical operation of the Galois group $\mathrm{G}_k(f)$ on K induces an operation of $\mathrm{G}_k(f)$ on the finite set $\mathrm{V}(f)=\{x_1,\dots,x_n\}$. Further, since any k-algebra homomorphism of K is uniquely determined by the images of the k-generators $x_1,\dots,x_n$, this induced operation of $\mathrm{G}_k(f)$ is also faithful, i. e. the substitution homomorphism $\mathrm{G}_k(f)\to\mathfrak{S}(\mathrm{V}(f))$, $\sigma\mapsto(x\mapsto\sigma(x))$ is an injective group homomorphism[19] and hence is a faithful representation of the Galois group $\mathrm{G}_k(f)$ of f

---

corresponding polynomial in $k'[X]$ (obtained by applying τ to the coefficients of f). Further, let $K|k$ (respectively, $K'|k'$) be splitting fields of f (respectively, f') over k (respectively, k'), then the isomorphism τ can be extended to an isomorphism $\rho:K\to K'$ such that $\rho(x)\in\mathrm{V}(f')$ for every $x\in\mathrm{V}(f)$.

This uniqueness allows us to use the term "*the* splitting field" of $f\in k[X]$ over k. The splitting fields of polynomials lead to an important property of field extensions, namely, the *normality* : An algebraic field extension $K|k$ is called normal if every irreducible polynomial in $g\in k[X]$ which has a zero in K splits completely in $K[X]$ into linear factors, or equivalently, if K contains a splitting field of f over k. An algebraic field extension $K|k$ is normal if and only if the minimal polynomial $\mu_{x,k}$ of every element $x\in K$ splits completely in $K[X]$ into linear factors, or equivalently, for every element $x\in K$ all the conjugates of x over k are also contained in K.

We note several important consequences of the definition of normal field extension: *Let $K|k$ be a finite normal field extension. Then:*

(1) *The field extension $K|k$ is a splitting field of some polynomial $f\in k[X]$ over k.*

(2) *If $x,y\in K$ are conjugates over k, then there exists a k-algebra automorphism $\sigma\in\mathrm{Gal}(K|k)$ such that $\sigma(x)=y$. In particular, if $g\in k[X]$ is an irreducible polynomial which has a zero in K, then the set of zeroes $\mathrm{V}(g)$ of g is contained in K and the Galois group $\mathrm{Gal}(K|k)$ operates transitively on $\mathrm{V}(g)$.* – This assertion played a crucial role in the development of Galois theory. See its use in the modern proof of the Lemma IV of [4] given in the Remark in the Footnote 19, see also Lemma 1.C.1.

(3) *If L is an intermediary subfield, then every k-algebra homomorphism $L\to K$ can be extended to a k-algebra automorphism of K, i. e. the restriction map $\mathrm{Gal}(K|k)\to\mathrm{Hom}_{k\text{-alg}}(L,K)$, $\sigma\mapsto\sigma|_L$ is surjective.*

The most important property of the splitting fields of polynomials is the converse of the assertion (1) above:

(4) *Any splitting field over k of a polynomial $f\in k[X]$ is a finite normal extension of k.* For a proof, we may assume that $f=(X-x_1)\cdots(X-x_n)$ is monic of degree $n\ge1$ and $K=k(x_1,\dots,x_n)$. Let $g\in k[X]$ be an irreducible polynomial over k and let $y\in K$ be a zero of g in K. To prove that g splits completely into linear factors in $K[X]$, we make use of the Fundamental Theorem on Symmetric Polynomials (see Footnote 22). Since $y\in K=k(x_1,\dots,x_n)=k[x_1,\dots,x_n]$ there exists a polynomial $\varphi(X_1,\dots,X_n)\in k[X_1,\dots,X_n]$ such that $y=\varphi(x_1,\dots,x_n)$. Consider the polynomial $\Phi(X):=\prod_{\sigma\in\mathfrak{S}_n}\big(X-\varphi(x_{\sigma(1)},\dots,x_{\sigma(n)})\big)\in K[X]$ which splits completely into linear factors in $K[X]$. Then $\Phi(X)\in k[X]$ by the Fundamental Theorem on Symmetric polynomials. Now, since $\Phi(y)=0$ and $g=\mu_{y,k}$ is the minimal polynomial over k, g must divide $\Phi(X)$ in $k[X]$ and hence g will also split completely into linear factors in $K[X]$. □

Finally, we note the following characteristic property of finite normal field extensions:

(5) *A finite field extension $K|k$ is normal over k if and only if it satisfies the following condition: if $K'|K$ is a field extension of K, then every k-algebra homomorphism $\sigma:K\to K'$ maps K into K.*

[19] This natural description of the Galois group $\mathrm{G}_k(f)$ goes back to Galois (see also Footnote 3 and Footnote 5 for a brief description of the passage from Galois' group to the modern Galois group $\mathrm{Gal}(K|k)=\mathrm{Aut}_{k\text{-alg}}K$). What is interesting is that Galois had no notion of automorphisms although automorphisms are implicit in his development of the theory. How did he decide which permutations in $\mathfrak{S}(\mathrm{V}(f))$ exactly form the Galois group $\mathrm{G}_k(f)$ of f? His approach was based on the primitive element (which we have called Galois resolvent of the splitting field $K=k(\mathrm{V}(f))$ of f, see 1.B.7) y of $K|k$ and its minimal polynomial $\mu_{y,k}\in k[X]$ which is separable, since $k(y)|k$ is a Galois extension. Let $y_1,\dots,y_m\in K$ be the zeroes of $\mu_{y,k}$ (all are in K) and $m=\deg(\mu_{y,k})=[K:k]=\#\,\mathrm{Gal}(K|k)=\#\mathrm{G}_k(f)$. Since $K=k(y)$, the zeroes $x_1,\dots,x_n$ of f can be expressed in the form $x_1=\varphi_1(y),\dots,x_n=\varphi_n(y)$ where $\varphi_1,\dots,\varphi_n\in k(Y)$ are rational functions in one indeterminate Y over k. Then the image of the canonical map $\mathrm{Gal}(K|k)\to\mathfrak{S}(\mathrm{V}(f))$ consists of the following permutations (these rows are used to denote the images of $x_1,\dots,x_n$; the elements in each row are distinct by the **Lemma:** (see [4, Lemma I, p.47]) *Let $\varphi\in k(X)$ be a rational function over k and let y be a zero of an irreducible polynomial $g\in k[X]$. If $\varphi(y)=0$, then $\varphi(z)=0$ for every zero z of g.*) which were described by Galois :

$$\begin{array}{rcccccc}
\mathrm{id} &=& \sigma_1 &=& \big(\varphi_1(y_1), & \varphi_2(y_1), & \dots, \quad \varphi_n(y_1)\big),\\
 & & \sigma_2 &=& \big(\varphi_1(y_2), & \varphi_2(y_2), & \dots, \quad \varphi_n(y_2)\big),\\
 & & \vdots & & \vdots & \vdots & \vdots \quad \vdots\\
 & & \sigma_m &=& \big(\varphi_1(y_m), & \varphi_2(y_m), & \dots, \quad \varphi_n(y_m)\big),
\end{array}$$

i. e. $\mathrm{Gal}(k(y)|k)=\{\sigma_1,\dots,\sigma_m\}$, where $\sigma_i:k(y)\to k(y)$ is the k-algebra automorphism of $k(y)$ defined by $\sigma_i(y)=y_i$, $i=1,\dots,m$. Under the canonical homomorphism $\mathrm{Gal}(k(y)|k)\to\mathfrak{S}(\mathrm{V}(f))$, σ_i is mapped to the permutation that takes $x_1=\varphi_1(y_1),\dots,x_n=$

in the permutation group $\mathfrak{S}_n$, $n = \deg(\mathrm{Red}\, f)$. This embedding of $\mathrm{G}_k(f)$ as a subgroup of $\mathfrak{S}_n$ depends on the numbering of the zeroes of f. Different numberings will give conjugate subgroups and hence one should be careful to formulate properties of $\mathrm{G}_k(f)$ as a subgroup of $\mathfrak{S}_n$ and take into account the possibility of conjugation. Further, *the orbits of the canonical operation of the Galois group* $\mathrm{G}_k(f)$ *on the zero set* $\mathrm{V}(f)$ *of* f *are precisely the zero sets* $\mathrm{V}(\pi_1),\ldots,\mathrm{V}(\pi_r)$*, where* $\pi_1,\ldots,\pi_r$ *are distinct prime divisors of* f. This is immediate from the following:

1.C.1 Lemma (Jordan[20]) *Let* $f \in k[X]$ *be a monic separable polynomial over k and let* $\mathrm{G}_k(f)$ *be the Galois group of* f *over k. Then the following are equivalent*:

(i) f *is irreducible over k.*

(ii) $\mathrm{G}_k(f)$ *acts transitively on the set* $\mathrm{V}(f)$ *of zeroes of* f *in the algebraic closure* $\bar{k}$ *of k.*

In particular, if $f \in k[X]$ *is an irreducible separable polynomial, then the degree* $\deg(f)$ *divides the order* $\#\mathrm{G}_k(f)$ *of the Galois group of* f *over k.*

Proof: Let K be the splitting field of f over k contained in the algebraic closure $\bar{k}$ of k. Then, since f is separable over k, $K|k$ is a Galois extension with Galois group $\mathrm{Gal}(K|k) = \mathrm{G}_k(f)$.

(i) $\Rightarrow$ (ii) : Since f is irreducible over k, it is the minimal polynomial $\mu_{x,k}$ of every $x \in \mathrm{V}(f)$. Therefore (by parts (4) and (2) in Footnote 18) for every $x, y \in \mathrm{V}(f)$ there exists $\sigma \in \mathrm{Gal}(K|k) = \mathrm{G}_k(f)$ such that $\sigma(x) = y$.

(ii) $\Rightarrow$ (i) : Let $x \in \mathrm{V}(f)$. Then, since $f(x) = 0$, $\mu_{x,k}$ divides f. Conversely, f divides $\mu_{x,k}$, since f is separable and every other $y \in \mathrm{V}(f)$ is a zero of $\mu_{x,k}$ because $\mu_{x,k}(y) = \mu_{x,k}(\sigma(x)) = \sigma(\mu_{x,k}(x)) = 0$ for some $\sigma \in \mathrm{G}_k(f)$ by (ii). □

Therefore, *the classification of the Galois operations defined by irreducible separable polynomials of degree n is equivalent to the classification of the conjugacy classes of the transitive subgroups of* $\mathfrak{S}_n$. See [6, Subsection 1.14] for the list of transitive subgroups of $\mathfrak{S}_n$, $n \leq 5$.

$\varphi_n(y_1)$ to $\sigma_i(\varphi_1(y_1)) = \varphi_1(y_i), \sigma_i(\varphi_2(y_1)) = \varphi_2(y_i), \ldots, \sigma_i(\varphi_n(y_1)) = \varphi_n(y_i)$, respectively, which is the i-th row displayed above. Finally, it is easy to check that the image does not depend on the choice of y and the rational functions $\varphi_1,\ldots,\varphi_n$.

Remark: The key property of the *Galois resolvent* y of f (Galois used a variation of Lagrange's notion of the resolvent polynomial, (see Footnote 36) and following Lagrange, he used the letter "V" for this resolvent "as function of the roots") is: *Every root of the given equation* f *can be expressed rationally as a function of y, i. e.* $K = k(x_1,\ldots,x_n) = k(y)$*, or equivalently,* y *is a primitive element of the splitting field of* f *over k.* This is the Lemma III of Galois' memoir [4, p. 49] which he submitted to the French Academy in 1831. Galois' proof was so terse that Simeon Denis Poisson (1781-1840) complained that the proof was insufficient but could be completed by using Lagrange's methods (see Lagrange's Rational Function Theorem in Footnote 36). In Galois' situation y is a root of the Galois resolvent polynomial which need not be irreducible over k. Galois made a crucial observation that the roots $y = y_1,\ldots,y_m \in K$ of the minimal polynomial $\mu_{y,k}$ of y over k interact with the roots of the original polynomial f: *If a rational function* $\varphi(y)$ *in* y *over k is one of the roots of* f*, then* $\varphi(y_2),\ldots,\varphi(y_m)$ *are also roots of* f. This was the Lemma IV in [4, p. 49-51]. For its proof, first note that, since $K|k$ is normal over k (see Footnote 18), $\mu_{y,k}$ splits completely over K, i. e. $y = y_1, y_2, \ldots, y_m \in K$. By (2) in Footnote 18, there exists $\sigma \in \mathrm{Gal}(K|k)$ such that $\sigma(y) = y_2$. Then the proof is immediate from the equalities $0 = \sigma(0) = \sigma(f(x)) = \sigma(f(\varphi(y))) = f(\sigma(\varphi(y))) = f(\varphi(\sigma(y))) = f(\varphi(y_2))$. Galois' proof of Lemma IV is different and it does not mention automorphisms explicitly. His proof is described in [3, pp. 51-52].

[20] It seems Galois knew this lemma, though Marie Ennemond Camille Jordan (1838-1922) was the first to state it explicitly. Jordan gave the first complete account of Galois Theory in 1870 in his text "*Traité des substitutions et des équations algébriques*", Gauthier Villars, Paris, 1870.

1.C.2 Corollary *Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial over $\mathbb{Q}$ which has at least one real and one non-real zero. Then the Galois group $\mathrm{G}_{\mathbb{Q}}$ of f is non-abelian.*

Proof: By assumption there are $x \in \mathbb{R}$ and $z \in \mathbb{C} \setminus \mathbb{R}$ which are zeroes of f. By Lemma 1.C.1 there exists $\tau \in \mathrm{G}_{\mathbb{Q}}(f)$ such that $\tau(x) = z$. This τ does not commute with the complex conjugation which is clearly an element of $\mathrm{G}_{\mathbb{Q}}(f)$. □

1.C.3 Example Let $n \in \mathbb{N}$, $n \geq 4$ and let $a, b \geq 2$ be square free natural numbers with $\gcd(a,b) \neq 1$. The the Galois groups $\mathrm{G}_{\mathbb{Q}}(X^n - a)$ and $\mathrm{G}_{\mathbb{Q}}(X^n \pm aX - b)$ are not abelian by 1.C.2.

1.C.4 Corollary *Let k be a field, $f \in k[X]$ and $f = a\pi_1^{\nu_1} \dots \pi_r^{\nu_r}$ be the prime factorisation of f in $k[X]$, where $a \in k^\times$, $\nu_1 \dots \nu_r$ are positive natural numbers and $\pi_1, \dots, \pi_r \in k[X]$ are distinct prime factors of f in $k[X]$. If $\operatorname{Red} f = \pi_1 \cdots \pi_r$ is separable, then the canonical group homomorphism $\mathrm{G}_k(f) \to \mathfrak{S}(\mathrm{V}(\pi_1)) \times \cdots \times \mathfrak{S}(\mathrm{V}(\pi_r))$ is injective.*

The index of $\mathrm{G}_k(f)$ in $\mathfrak{S}(\mathrm{V}(f))$ is called the affect[21] of f. If this is 1, i. e. if $\mathrm{G}_k(f) = \mathfrak{S}(\mathrm{V}(f))$ then f is also called a polynomial without affect or affect-free polynomial. A reduced polynomial without affect is necessarily irreducible. Explicit examples of affect-free polynomials (over $\mathbb{Q}$) are given at the end of Section 3.

1.C.5 Example (Galois group of the general equation) Let k be an arbitrary field and let $f_n := (X - X_1)(X - X_2) \cdots (X - X_n) = X^n + \sum_{j=1}^{n} (-1)^j \mathrm{S}_j X^{n-j}$ be the general monic polynomial of degree n over k, where $\mathrm{S}_j := \sum_{1 \leq i_1 < i_2 < \cdots < i_n \leq n} X_{i_1} X_{i_2} \cdots X_{i_n}$, $j = 1, \dots, n$, are elementary symmetric polynomials in $X_1, \dots, X_n$. We consider f_n as a polynomial in X over the (fixed) subfield $K^{\mathfrak{S}_n} := k(\mathrm{S}_1, \dots, \mathrm{S}_n)$ of the field $K := k(X_1, \dots, X_n)$ of rational functions in $X_1, \dots, X_n$ over k and say that $f_n(x) = 0$ is the general equation of degree n over k. The field extension $K | K^{\mathfrak{S}_n}$ is the splitting field of the separable polynomial $f_n \in K^{\mathfrak{S}_n}[X]$ and is called the general Galois extension of degree n. Moreover,we have the natural isomorphism of groups $\mathrm{Gal}(K | K^{\mathfrak{S}_n}) \xrightarrow{\sim} \mathfrak{S}_n$.[22] Further, the fixed field $K^{\mathfrak{A}_n}$ of the *alternating group*[23] $\mathfrak{A}_n$ is the subfield $K^{\mathfrak{S}_n}(\Delta_f)$ generated by the square root Δ_f of the discriminant $\operatorname{Disc} f_n$ over $K^{\mathfrak{S}_n}$ and $\mathrm{Gal}(K | K^{\mathfrak{A}_n}) = \mathfrak{A}_n$.

1.C.6 Example (Cyclic extensions and pure equations) A Galois extension $K | k$ is called cyclic if its Galois group $\mathrm{Gal}(K | k)$ is a cyclic group. Let $K | k$ be a cyclic Galois extension of degree n and let σ be a generator of the Galois group $\mathrm{Gal}(K | k)$. We give

---

[21] The term "affect" in this context was introduced by Kronecker. Instead of "affect" Weber used the term "degree of the affect".

[22] From the modern point of view this is best stated using the language of group actions. The symmetric group $\mathfrak{S}_n$ operates canonically on the polynomial ring $k[X_1, \dots, X_n]$ as: for $\sigma \in \mathfrak{S}_n$ and for $f \in k[X_1, \dots, X_n]$, let σf be the polynomial obtained from f by permuting the variables according to σ, i. e. $\sigma f(X_1, \dots, X_n) := f(X_{\sigma 1}, \dots, X_{\sigma n})$. Further, the map $k[X_1, \dots, X_n] \to k[X_1, \dots, X_n]$, $f \mapsto \sigma f$ is a k-algebra automorphism and hence it extends to an automorphism $\tilde{\sigma}$ of its field of fractions $k(X_1, \dots, X_n)$. Moreover, the set of fixed elements $K^{\mathfrak{S}_n}$ of this operation of $\mathfrak{S}_n$ are precisely the elements of $k(\mathrm{S}_1, \dots, \mathrm{S}_n)$ and hence the notation $K^{\mathfrak{S}_n}$. Although this is stated in modern language the content is precisely the classical Fundamental Theorem on Symmetric Polynomials which states that: *every symmetric polynomial in $X_1, \dots, X_n$ is a polynomial in elementary symmetric polynomials* $\mathrm{S}_1, \dots, \mathrm{S}_n$. This fact goes back to Sir Isaac Newton (1643-1727) and was used freely by the predecessors of Galois. This proves that the group homomorphism $\mathrm{Gal}(K | K^{\mathfrak{S}_n}) \to \mathfrak{S}_n$ is surjective and hence an isomorphism (see 1.C). Therefore the Galois theory of the general equation of degree n was already known to Lagrange, Paolo Ruffini (1765-1822) and Niels-Henrik Abel (1802-1829), see also Footnotes 34 and 35. What was missing was the notion of *normal subgroup* as it was not visible in their work and hence they could not formulate the notion of a *solvable group*. The rudiments of group theory play a big role in Abel's work but the normal subgroups make no appearance.

[23] The isotropy group $\mathrm{G}_{\Delta_{f_n}}$ of Δ_{f_n} is called the alternating group on $\{1, \dots, n\}$, usually denoted by $\mathfrak{A}_n$. This was the definition of the alternating group during the time of Lagrange, Ruffini, Cauchy and Abel. Δ_{f_n} depends on the indexing of the roots $X_1, \dots, X_n$ of f_n; new indexing may change the sign of Δ_{f_n}. The signature $\operatorname{Sign}\sigma$ of a permutation $\sigma \in \mathfrak{S}_n$ is then defined by the formula : $\sigma(\Delta_{f_n}) = (\operatorname{Sign}\sigma)\Delta_{f_n}$.

a relation between the following two endomorphisms, namely, the norm $\mathrm{N} := \mathrm{N}_k^K : K \to k \subseteq K$, $x \mapsto \mathrm{N}_k^K(x) = \prod_{i=0}^{n-1} \sigma^i(x)$ and $\sigma/\mathrm{id}_K : K^\times \to K^\times$, $x \mapsto \sigma(x)/x$ of the multiplicative group $K^\times$ of the field K:

(Hilbert Theorem 90[24]– Multiplicative form) *The sequence* $K^\times \xrightarrow{\sigma/\mathrm{id}} K^\times \xrightarrow{\mathrm{N}} K^\times$ *is exact.* **Proof:** Clearly $\mathrm{N} \circ (\sigma/\mathrm{id})(x) = \mathrm{N}(\sigma(x)/x) = \mathrm{N}(\sigma(x))/\mathrm{N}(x) = 1$ for every $x \in K$, i. e. $\mathrm{N} \circ (\sigma/\mathrm{id})$ is trivial. Conversely, let $y \in K^\times$ be such that $\mathrm{N}(y) = 1$. Since $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ are linearly independent over K by the Dedekind-Artin Lemma (see Footnote 6), the k-linear endomorphism $\rho := \sum_{i=0}^{n-1} \left(\prod_{j=0}^{i-1} \sigma^j(y^{-1}) \right) \sigma^i$ of K is non-zero. Further, since $1 = \mathrm{N}(y^{-1}) = \prod_{j=0}^{n-1} \sigma^j(y^{-1})$, clearly $y^{-1}\sigma\rho = \rho$ and hence $y = \sigma\rho(z)/\rho(z)$ for every $z \in K$ with $\rho(z) \neq 0$. □

Remark: In general the sequence $K^\times \xrightarrow{\mathrm{N}} K^\times \xrightarrow{\sigma/\mathrm{id}} K^\times$ is not exact. Moreover, the composition $(\sigma/\mathrm{id}) \circ \mathrm{N}$ is the trivial homomorphism, but the homology group $\mathrm{Ker}(\sigma/\mathrm{id})/\mathrm{Im}\,\mathrm{N}$ is the norm residue group $K^\times/\mathrm{N}(K^\times)$. For example, $\mathbb{R}^\times/\mathrm{N}(\mathbb{C}^\times) \cong \mathbb{Z}^\times$.

Let $n \in \mathbb{N}^+$ and let k be a field of characteristic $p \geq 0$ which does not divide n. Suppose that k contains all n-th roots of unity. Then

(1) *The Galois group of a pure irreducible separable polynomial* $X^n - c \in k[X]$, $c \neq 0$, *is cyclic of order* n. In fact, for any zero x of $X^n - c$, the map $\mathrm{G}_k(X^n - c) \to \mathbf{W}_n$, $\sigma \mapsto \sigma(x)/x$ is an isomorphism of groups, where $\mathbf{W}_n = \mathbf{W}_n(k)$ (see Footnote 10) is the cyclic group of n-th roots of unity in k. – Moreover, this isomorphism is independent of the choice of the zero x and therefore is a canonical isomorphism.

(2) Conversely, *if* $K|k$ *is a cyclic Galois extension of degree* n, *then* K *is a minimal splitting field of a pure polynomial* (necessarily irreducible) $X^n - c \in k[X]$. For a proof, let $\zeta \in k$ be a primitive n-th root of unity and let σ be a generator of the Galois group $\mathrm{Gal}(K|k)$. In view of the proof of (1), we need to find an element $x \in K$ such that $\sigma(x)/x = \zeta$. This is possible by Hilbert Theorem 90, since $\mathrm{N}_k^K(\zeta) = \mathrm{Det}(\lambda_\zeta) = \zeta^n = 1$. Then $\sigma(x^n) = (\sigma(x))^n = (\zeta x)^n = x^n$ and hence $c := x^n$ is an element of k. Further, the polynomial $X^n - c \in k[X]$ splits completely in K, since all the n distinct zeroes $\zeta^i x = \sigma^i(x)$, $i = 0, \ldots, n-1$ are in K. Moreover, $\mathrm{Gal}(K|k)$ operates transitively on the set of zeroes $\mathrm{V}(X^n - c)$ of $X^n - c$ and hence $X^n - c$ is irreducible over k by 1.C.1. □

1.C.7 Example (Galois group of pure equations) Let k be a field, $n \in \mathbb{N}$ be a positive natural number which is coprime to $\mathrm{Char}\,k$ and let $f = X^n - c \in k[X]$, $c \neq 0$. Let K be a (minimal) splitting field of f over k and let L be a (minimal) splitting field of $X^n - 1$ over k contained in K. If $x \in K$ be an arbitrary zero of f, then $K = L(x)$ and the map $\mathrm{G}_k(f) = \mathrm{Gal}(K|k) \to \mathbf{W}_n \rtimes \mathrm{Aut}\,\mathbf{W}_n$ defined by $\sigma \mapsto (\sigma(x)/x, \sigma|\mathbf{W}_n)$ is an injective group homomorphism, where $\mathbf{W}_n := \mathbf{W}_n(L)$ (see Footnote 10). In particular, the Galois group $\mathrm{G}_k(f)$ of f is solvable, since it is a subgroup of the solvable group[25] $\mathbf{W}_n \rtimes \mathrm{Aut}\,\mathbf{W}_n$.

---

[24] This theorem of David Hilbert (1862-1943) is the 90-th Theorem from the well-known *Zahlbericht im Jahresbericht der Deutschen Mathematiker-Vereinigung* **4** (1897).

[25] *The (full) holomorph of (the cyclic group)* $\mathbf{W}_n$ *is the semidirect product* $\mathbf{L}_n := \mathbf{W}_n \rtimes \mathrm{Aut}\,\mathbf{W}_n$ *and it is solvable.* For a proof note that $N := \mathbf{W}_n \times \{\mathrm{id}\}$ is a normal subgroup ($\cong \mathbf{W}_n \cong (\mathbf{Z}_n, +)$) and $H := \{1\} \times \mathrm{Aut}\,\mathbf{W}_n \cong (\mathbb{Z}_n)^\times$. Therefore from the short exact sequence $0 \to N \to \mathbf{L}_n \to H \to 0$, it follows that $\mathbf{L}_n$ is a solvable group of order $n\varphi(n)$. – The group $\mathbf{L}_n$ is isomorphic to the group of linear automorphisms of $\mathbb{Z}_n[X]$ and hence also known as a (full) linear group. Let ζ be a generator (primitive n-th root of unity) of $\mathbf{W}_n$. Then the map $(u, \Phi) \mapsto (X \mapsto aX + r)$ is an isomorphism of groups, where r and a are uniquely determined by the equations $u = \zeta^r$ and $\Phi(\zeta) = \zeta^a$, respectively. – Recall that a finite group G is solvable if there is a sequence of subgroups $\{1\} = G_m \subsetneq G_{m-1} \subsetneq \cdots \subsetneq G_0 = G$ such that for each $i = 1, \ldots, m$, G_i is normal in G_{i-1} and $p_i = [G_{i-1} : G_i]$ is a prime number. Subgroups and quotient groups of a solvable group are solvable. Finite abelian groups are solvable. In some cases the solvability of a group is determined just by its order. For example, *every group of a prime power order is solvable.* In 1904 William Burnside (1852-1927) generalized this to: *every group of order* $p^n q^m$, *where* p *and* q *are distinct primes, are solvable.* In 1963, Walter Feit (1930-2004) and John Griggs Thompson (1932-) proved the following surprising result: *every group of odd order is solvable.* This is a highly non-trivial theorem and its proof involves very sophisticated mathematics consisting of 255 pages.

Let $f(t) \in \mathbb{Q}[t]$ be a non-constant separable polynomial which splits into linear factors over $\mathbb{Q}$. Then the Galois group $G_{\mathbb{Q}(t)}(X^n - f(t))$ is not abelian (use similar argument as in 1.C.2). But the Galois group $G_{\mathbb{C}(t)}(X^n - f(t))$ is in fact, cyclic of order n.

1.C.8 Example (Cyclic extensions and Artin-Schreier[26] equations) Let $K|k$ be a cyclic Galois extension of degree n and let σ be a generator of the Galois group $\mathrm{Gal}(|k)$. Then the trace form $\mathrm{tr} = \mathrm{tr}_k^K : K \to k$ is $\mathrm{tr} = \sum_{i=0}^{n-1} \sigma^i$ and the additive counterpart of the above Hilbert Theorem 90 is:

(Hilbert Theorem 90 – Additive form) *The sequence* $K^\times \xrightarrow{\sigma - \mathrm{id}} K^\times \xrightarrow{\mathrm{tr}} K^\times$ *is exact.* **Proof:** Clearly $\mathrm{tr} \circ (\sigma - \mathrm{id})(x) = \mathrm{tr}(\sigma(x) - x) = \mathrm{tr}(\sigma(x)) - \mathrm{tr}(x) = 0$ for every $x \in K$, i. e. $\mathrm{tr} \circ (\sigma - \mathrm{id})$ is trivial. Conversely, let $y \in K^\times$ be such that $\mathrm{tr}(y) = 0$. Consider $\theta := \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i-1} \sigma^j(y) \right) \sigma^i$ of K is non-zero. Since $0 = \mathrm{tr}(y) = \sum_{i=0}^{n-1} \sigma^i(y)$, clearly $-y\,\mathrm{tr} + \sigma\theta = \theta$. By Dedekind-Artin Lemma $\mathrm{tr} \neq 0$ and hence for every $z \in K$ with $\mathrm{tr}(z) \neq 0$ we have $y = \sigma(\theta(z)/\mathrm{tr}(z)) - \theta(z)/\mathrm{tr}(z)$. □

Remark: The sequence $K^\times \xrightarrow{\mathrm{tr}} K^\times \xrightarrow{\sigma - \mathrm{id}} K^\times$ is always exact. This follows immediately from the fact that the trace map tr is k-linear and (since $\mathrm{tr} \neq 0$) has image k.

In the critical case of Galois extensions of degree p of a field of characteristic $p > 0$, the Artin-Schreier polynomials are used to replace the pure polynomials. See, for example, the next subsection.

Let k be a field of characteristic $p > 0$.

(1) *The polynomial* $X^p - X - c \in k[X]$, $c \neq 0$ *either factors into linear factors over* k*, or is irreducible over* k*. Moreover, in the latter case, its Galois group is cyclic of order* p*.* In fact, for any zero x of $X^p - X - c$, the map $G_k(X^p - X - c) \to \mathbf{Z}_p$, $\sigma \mapsto \sigma(x) - x$ is an isomorphism

---

The definition of the solvability of a group is closely related to the ideas of *simple groups*. – A group G is called simple if its only normal subgroups are the trivial subgroups $\{e\}$ and G. For example, the cyclic groups of prime order are simple. The term "simple group" is due to Jordan. He was the first to prove that: *the alternating group* $\mathfrak{A}_n$ *is simple for* $n \geq 5$. The simplicity of $\mathfrak{A}_5$ is also implicit in the work of Ruffini and Abel on the unsolvability of the quintic equation. Observe that non-abelian finite simple groups are not solvable and hence there are many non-solvable groups. *The alternating group* $\mathfrak{A}_n$ *and the symmetric group* $\mathfrak{S}_n$ *are solvable if and only if* $n \leq 4$. With this we can determine the normal subgroups of $\mathfrak{S}_n$, they are precisely: $\{e\}$, $\mathfrak{A}_n$ and $\mathfrak{S}_n$.

The relation between simple and solvable groups is even more interesting. The key observation is that all finite groups are "built" by using simple groups by means of *composition series*. – if G is a finite group, then a composition series of G is a sequence $\{e\} = G_{m-1} \subsetneq G_{m-1} \subsetneq \cdots \subsetneq G_1 \subsetneq G_0 = G$ such that G_i is normal in G_{i-1} and the quotient group G_{i-1}/G_i is simple for all $i = 1, \ldots, m$. The simple quotient groups G_{i-1}/G_i, $i = 1, \ldots, m$, are called the composition factors of G. For example, for $n \geq 5$, $\{e\} \subsetneq \mathfrak{A}_n \subsetneq \mathfrak{S}_n$ is a composition series of $\mathfrak{S}_n$. A given finite group may have more than one composition series, for example, the sequences $\{e\} \subsetneq \mathrm{H}([2]) \subsetneq \mathbf{Z}_6$ and $\{e\} \subsetneq \mathrm{H}([3]) \subsetneq \mathbf{Z}_6$ are composition series of the cyclic group $\mathbf{Z}_6$. However, the composition factors are $\mathbf{Z}_3$, $\mathbf{Z}_2$ (respectively, $\mathbf{Z}_2$, $\mathbf{Z}_3$). The Jordan-Hölder Theorem asserts that: *Any two composition series of a finite group have the same length and that the corresponding composition factors are isomorphic upto a permutation.* Therefore the quotient groups in a composition series of a group are the simple groups from which the group is built. In particular, a finite group is solvable if and only if its composition factors are the "simplest" simple groups, namely the abelian ones. The idea of a composition series is due to Jordan. He proved that any two composition series of a group have the same length and that the indices $[G_{i-1} : G_i]$ are unique upto a permutation. Once the concept of the quotient group was better understood, Otto Ludwig Hölder (1859-1937) proved the Jordan-Hölder theorem.

The simple groups coming from finite fields were first studied by Jordan. In 1870 he gave an incomplete proof that: *The special projective linear group* $\mathrm{PSL}(n, \mathbb{F}_p)$ *of* $\mathbb{F}_p^n$ *is simple except* $n = 2$ *and* $p = 2$ *or* 3. In this proof Jordan used the *Jordan canonical form* to study matrices in the general linear group $\mathrm{GL}(n, \mathbb{F}_p)$. The canonical form uses the eigenvalues of the matrix which are the zeroes of the characteristic polynomial and hence the eigenvalues lie in finite field extensions of $\mathbb{F}_p$. This shows that more general finite fields arise naturally while studying the group $\mathrm{GL}(n, \mathbb{F}_p)$. Jordan further studied the groups $\mathrm{GL}(n, \mathbb{F}_{p^m})$. The complete proof of the above assertion was given by Leonard Eugene Dickson (1874-1954) in 1897.

It is proved in 2.1 that the one dimensional affine linear group $\mathrm{Aff}(\mathbb{F}_p)$ over $\mathbb{F}_p$ is solvable. In the early twentieth century this affine group was called "metacyclic". These days the term "metacyclic" is used more generally for any group G which has a normal subgroup N such that both N and the quotient group G/N are cyclic. In group theory this notion was introduced by Ferdinand Georg Frobenius (1849-1917).

[26] This Example goes back to Artin and Otto Schreier (1901-1929) and therefore polynomials of the type $X^p - X - c$ over a field k of characteristic $p > 0$ are called Artin-Schreier polynomials.

of groups and hence its Galois group is cyclic of order p. Moreover, this isomorphism is independent of the choice of a zero x and therefore is a canonical isomorphism.

(2) Conversely, *if $K|k$ is a cyclic Galois extension of degree p, then K is a minimal splitting field of a polynomial* (necessarily irreducible) $X^p - X - c \in k[X]$. For a proof, let σ be a generator of the Galois group $\mathrm{Gal}(K|k)$. In view of the proof of (1), we need to find an element $x \in K$ such that $\sigma(x) - x = 1$. This is possible by Hilbert Theorem 90 (additive form), since $\mathrm{tr}_k^K(1) = p \cdot 1 = 0$. Then $\sigma(x^p - x) = (\sigma(x))^p - \sigma(x) = (x+1)^p - (x+1) = x^p - x$ and hence $c := x^p - x$ is an element of k. Further, since $x \notin k$, $K = k(x)$ and the polynomial $X^p - X - c \in k[X]$ is the minimal polynomial of x over k. □

1.C.9 Example (Equations with Galois group $\mathbf{Q}$ – The Quaternion group) Let $\mathbf{Q} := \{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$ denote the quaternion group of order 8. All proper subgroups of $\mathbf{Q}$ are normal, abelian and their factor groups are also abelian. Let $\sqrt{2}, \sqrt{3}$ denote the positive square roots of $2, 3$, respectively and let $\alpha := (1+\sqrt{2})(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3} \in \mathbb{R}$, $L := \mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Further, let $\omega := \sqrt{\alpha} \in \mathbb{R}$ be the positive square root of α and let $K := L(\omega) = \mathbb{Q}(\omega)$. Then $K|\mathbb{Q}$ is a Galois field extension with Galois group $\mathbf{Q}$. It is easy to check that the minimal polynomial $\mu_{\omega,\mathbb{Q}} \in \mathbb{Q}[X]$ is $\mu_{\omega,\mathbb{Q}} = X^8 - 24X^6 + 108X^4 - 144X^2 + 36 \in \mathbb{Q}[X]$ and the Galois group $\mathrm{G}_{\mathbb{Q}}(\mu_{\omega,\mathbb{Q}})$ over $\mathbb{Q}$ is $\mathbf{Q}$. – This is the simplest equation (over $\mathbb{Q}$) with Galois group $\mathbf{Q}$. Moreover, every equation $f(x) = 0$ over a field k with separable reduction and $\mathrm{G}_k(f) = \mathbf{Q}$ has a prime factor g of degree 8 with $\mathrm{G}_k(g) = \mathbf{Q}$. For a proof, it is enough to prove that the canonical operation of $\mathbf{Q}$ on the set of zeroes $\mathrm{V}(f)$ has at least one orbit of cardinality 8. Let $\mathrm{H} := \mathrm{H}(\mathrm{i}) \subseteq \mathbf{Q}$ be the subgroup generated by i. Then, since $\mathrm{ord}\,\mathrm{i} = 4$, it follows that the restriction of the operation of $\mathbf{Q}$ to H on the set of zeroes $\mathrm{V}(f)$ has at least one orbit $\mathrm{H}x$ of cardinality 4. Then $\mathbf{Q}$-orbit of x has cardinality 8, since $\{\pm 1\}$ is the only subgroup of $\mathbf{Q}$ of index 4 which is also a subgroup of H.

When exactly the Galois group of an equation is a subgroup of the alternating group, can be answered in the following:

1.C.10 Lemma *Let k be a field of characteristic $\neq 2$ and let $f \in k[X]$ be a polynomial with separable reduction* $\mathrm{Red}\, f$. *Then the Galois group* $\mathrm{G}_k(f)$ *is contained in the alternating group if and only if the discriminant* $\mathrm{Disc}(\mathrm{Red}\, f)$ *is a square in k.*

Proof: Without loss of generality we may assume that $f = \mathrm{Red}\, f$ and $n = \deg f > 1$. Let $x_1, \ldots, x_n$ be the distinct zeroes of f. Then $\mathrm{Disc}\, f = a^{2n-2}\mathrm{V}^2$, where $a \in k^\times$ is the leading coefficient of f and $\mathrm{V} := \mathrm{V}(x_1, \ldots, x_n)$ is the Vandermonde determinant of $x_1, \ldots, x_n$. For every $\sigma \in \mathrm{G}_k(f)$, we have $\sigma\mathrm{V} = \mathrm{V}(\sigma(x_1), \ldots, \sigma(x_n)) = (\mathrm{sign}\,\sigma)\mathrm{V}$. Therefore, since $\mathrm{V} \neq 0$ and $2 \neq 0$ in k, it follows that $\mathrm{G}_k(f) \subseteq \mathfrak{A}_n$ if and only if V is invariant under all $\sigma \in \mathrm{G}_k(f)$, i. e. $\mathrm{V} \in K^{\mathrm{G}_k(f)} = k$, or equivalently, $\mathrm{Disc}\, f = (a^{n-1})^2\mathrm{V}^2$ is a square in k. □

The above proof also shows that if characteristic of k is 2, then the discriminant of an equation is always a square in k.

If $\mathrm{Disc}(\mathrm{Red}\, f)$ is not a square in k, then $k[\mathrm{V}]$ is a quadratic field extension of k and the corresponding subgroup of $\mathrm{G}_k(f)$ is the normal subgroup of index 2 and coincides with the intersection of $\mathrm{G}_k(f)$ and the alternating group $\mathfrak{A}_n$.

1.C.11 Example (Galois groups of equations of degree ≤ 3) Let us consider the special equations of degree 2 and 3 over a field k of characteristic $\neq 2$. For an irreducible separable quadratic polynomial $f = aX^2 + bX + c$ over k, we have $\mathrm{G}_k(f) = \mathfrak{S}_2$ if and only if $\mathrm{Disc}\, f = b^2 - 4ac$ is not a square in k. This matches with the Lemma 1.C.10. For an irreducible

separable cubic polynomial f over k, the only possibilities for the Galois group $\mathrm{G}_k(f)$ are $\mathfrak{A}_3$ and $\mathfrak{S}_3$ and by Lemma 1.C.10 the decision can be made only by using the discriminant $\mathrm{Disc}\, f$.

1.C.12 Example Let $f := X^4 - 4X + 2 \in \mathbb{Q}[X]$. Then f is irreducible over $\mathbb{Q}$ by the Schönemann-Eisenstein criterion. Further, $f = (X-x)(X+x)(X-y)(X+y)$ and $\mathrm{V}(f) = \{\pm x, \pm y\}$, where $x = \sqrt{2+\sqrt{2}}$ and $y = \sqrt{2-\sqrt{2}}$ and hence $K = \mathbb{Q}(x,y)$ is the splitting field of f over $\mathbb{Q}$. Further, $[K:\mathbb{Q}] \geq 8$, since $y \notin \mathbb{Q}(x)$. The transposition $\tau := \langle x, y\rangle \in \mathfrak{S}(\pm x, \pm y)$ is not an element of the Galois group $\mathrm{G}_{\mathbb{Q}}(f)$, since if $\tau(x) = y$, then we must also have $\tau(-x) = -\tau(x) = -y$. This means that the transposition τ does not respect the algebraic structure of the zeroes of f and hence it is not in the image of the canonical injective group homomorphism $\mathrm{Gal}(K|k) \to \mathfrak{S}(\mathrm{V}(f))$, i. e. τ is not the restriction of an automorphism of the splitting field K over k. We can use Lemma 1.C.1 and Lemma 1.C.10 to compute the Galois group $\mathrm{G}_{\mathbb{Q}}(f)$ over $\mathbb{Q}$. First, by Lemma 1.C.1 $\mathrm{G}_{\mathbb{Q}}(f)$ is a transitive subgroup of $\mathfrak{S}(\pm x, \pm y) = \mathfrak{S}_4$. Moreover, $\mathrm{Disc}\, f = (4xy)^2(x-y)^4(x+y)^4 = 2^8 \cdot 2^2 \cdot 2$ is not a square in $\mathbb{Q}$ and hence $\mathrm{G}_{\mathbb{Q}}(f) \not\subseteq \mathfrak{A}_4$ by Lemma 1.C.10. Therefore (by the list given in [6, Subsection 1.14]) $\mathrm{G}_{\mathbb{Q}}(f) = \mathbf{D}_4$ (= the dihedral group of order 8).

1.C.13 Example (Galois groups of equations of degree 4) Let k be a field and let $f = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in k[X]$ be a monic irreducible separable polynomial over k. Further, let x_1, x_2, x_3, x_4 be the (distinct) zeroes of f and $K = k(x_1, x_2, x_3, x_4)$ be the splitting field of f over k. Then the degree $[K:k] = \#\,\mathrm{Gal}(K|k) = \#\mathrm{G}_k(f)$ is a multiple of 4. Using x_1, x_2, x_3, x_4 we define $y_1 := x_1x_4 + x_2x_3$, $y_2 := x_1x_3 + x_2x_4$, $y_3 := x_1x_2 + x_3x_4$. Then we have

$$\mathrm{V}(x_1, x_2, x_3, x_4) = (y_1 - y_2)(y_3 - y_1)(y_3 - y_2) = \mathrm{V}(y_1, y_2, y_3)\,.$$

All permutations of x_1, x_2, x_3, x_4 clearly permute y_1, y_2, y_3 as well. Therefore elementary symmetric functions in y_1, y_2, y_3 are symmetric polynomials in x_1, x_2, x_3, x_4 which are polynomials in a_1, a_2, a_3, a_4 with coefficients in k and hence belong to k. Further, the cubic polynomial

$$g := (Y - y_1)(Y - y_2)(Y - y_3)$$

belongs to $k[Y]$; in fact, one can easily check that

$$g = Y^3 - a_2Y^2 + (a_1a_3 - 4a_4)Y - a_1^2a_4 + 4a_2a_4 - a_3^2\,.$$

The cubic resolvent $g \in k[Y]$ defined above is called a cubic resolvent of f. It follows immediately from $\mathrm{V}(x_1, x_2, x_3, x_4) = \mathrm{V}(y_1, y_2, y_3)$ that $\mathrm{Disc}\, f = \mathrm{Disc}\, g$.

Instead of y_1, y_2, y_3 one can also use $y_1 + y_2$, $y_1 + y_3$, $y_2 + y_3$ or similar symmetric terms, to get similar but different cubic resolvents. However, in our discussion below we use our special construction given above and hence g will be called *the* cubic resolvent of f. The splitting field of g over k is the intermediary field $L := k(y_1, y_2, y_3)$ of $K|k$; its degree $[L:k] \leq 6$ and hence $K \supsetneq L \supseteq k$. Further, since $\mathrm{D} := \mathrm{Disc}\, g = \mathrm{Disc}\, f \neq 0$, g is separable, i. e. y_1, y_2, y_3 are distinct. With this information, it follows easily that:

$$\mathrm{Gal}(K|k) \cap \mathbf{V}_4 = \mathrm{Gal}(K|L) \text{ and } \mathrm{G}_k(g) = \mathrm{G}_k(f)/\mathrm{G}_k(f) \cap \mathbf{V}_4\,,$$

where $\mathbf{V}_4 := \{\mathrm{id}, \langle 1,2\rangle\langle 3,4\rangle, \langle 1,3\rangle\langle 2,4\rangle, \langle 1,4\rangle\langle 2,3\rangle\}$ denotes the Klein's 4-group (in $\mathfrak{S}_4$). The Vandermonde determinant $\mathrm{V}(x_1, x_2, x_3, x_4)$ belongs to L and hence D is a square in L.

We assume that k is a field of characteristic $\neq 2$. Then:

(a) $\mathrm{G}_k(f) = \mathfrak{S}_4$ if and only if $g(Y)$ is irreducible over k and $\mathrm{Disc}(f)$ is not a square in k.
(b) $\mathrm{G}_k(f) = \mathfrak{A}_4$ if and only if $g(Y)$ is irreducible over k and $\mathrm{Disc}(f)$ is a square in k.
(c) $\mathrm{G}_k(f) = \mathbf{V}_4$ if and only if $g(Y)$ splits into linear factors over k.
(d) $\mathrm{G}_k(f) = \mathbf{Z}_4$ if and only if $g(Y)$ has exactly one zero $z \in k$ and the polynomial $F := F_1 \cdot F_2 \in k[X]$ splits into linear factors over L, where $F_1 := X^2 - zX + a_4$, $F_2 := X^2 + a_1X + (a_2 - z) \in k[X]$, or equivalently, $\mathrm{Disc}\, F_1 = z^2 - 4a_4$ and $\mathrm{Disc}\, F_2 = a_1^2 - 4(a_2 - z)$ are squares in L.

(e) $G_k(f) = \mathbf{D}_4$ if and only if $g(Y)$ has exactly one zero $z \in k$ and the polynomial $F := F_1 \cdot F_2 \in k[X]$ does not split into linear factors over L, where $F_1 := X^2 - zX + a_4$, $F_2 := X^2 + a_1X + (a_2 - z) \in k[X]$, or equivalently, at least one of $\mathrm{Disc}\, F_1 = z^2 - 4a_4$ and $\mathrm{Disc}\, F_2 = a_1^2 - 4(a_2 - z)$ is not a square in L.

Finally, we illustrate the above results by the following concrete examples:

(1) Let $f := X^4 + bX^2 + c \in k[X]$ be a biquadratic separable irreducible polynomial over k. Then b is a zero of the cubic resolvent $g = Y^3 - bY^2 - 4cY + 4bc = (Y - b)(Y^2 - 4c)$ of f and $\mathrm{Disc}(f) = \mathrm{Disc}(g) =^{27} h(a)^2 \cdot \mathrm{Disc}(h) = (b^2 - 4c)^2 \cdot 16c$, where $h := g/(Y - b) = Y^2 - 4c$. Therefore the Galois group $G_k(f)$ is one of the groups $\mathbf{D}_4, \mathbf{Z}_4$ or $\mathbf{V}_4$. Moreover, $G_k(f) = \mathbf{V}_4$ if and only if $\mathrm{Disc}(f)$ is a square in k, or equivalently, c is a square in k. If c is not a square in k, then b is the only zero of g in k, $L = k(\sqrt{c})$ and $F = (X^2 - bX + c)X^2$. Therefore F splits into linear factors over L if and only if [28] $(b^2 - 4c)c$ is a square in k and hence $G_k(f) = \mathbf{Z}_4$ or $\mathbf{D}_4$ according as $(b^2 - 4c)c$ is a square in k or not.

Let p, q be distinct odd prime numbers and let $f = X^4 - pX^2 + q \in \mathbb{Q}[X]$. Then f is irreducible over $\mathbb{Q}$, since $p^2 - 4q$ is not a square in $\mathbb{Q}$. Further, since both q and $q(p^2 - 4q)$ are not squares in $\mathbb{Q}$, it follows that $G_{\mathbb{Q}}(f) = \mathbf{D}_4$.

Let $m, n \in \mathbb{Z}$ be such that $m^2 + n^2$ is not a square in $\mathbb{Q}$. Then the Galois group of the polynomial $f = X^4 - 2(m^2 + n^2)X^2 + n^2(m^2 + n^2)$ is $\mathbf{Z}_4$, since $4m^2n^2(m^2 + n^2)^2$ is a square in $\mathbb{Q}$.

(2) Let $f = X^4 + aX^3 + bX^2 + aX + 1 \in k[X]$ be a self-reciprocal separable irreducible polynomial over k (and hence the rational function $f/(X + X^{-1})$ is a polynomial in $(X + X^{-1})$). Then 2 is a zero of the cubic resolvent

$$g = Y^3 - bY^2 + (a^2 - 4)Y + 4b - 2a^2 = (Y - 2)(Y^2 + (2 - b)Y + a^2 - 2b)$$

of f and $\mathrm{Disc}(f) = \mathrm{Disc}(g) =^{28} h(2)^2 \cdot \mathrm{Disc}(h) = (8 - 4b + a^2)^2(2 + 2a + b)(2 - 2a + b)$ $= (8 - 4b + a^2)^2 f(1) f(-1)$, where $h = g/(Y - 2) = Y^2 + (2 - b)Y + a^2 - 2b$. Therefore the Galois group $G_k(f)$ is $\mathbf{V}_4$ if and only if $\delta := f(1)f(-1) = (b + 2)^2 - 4a^2$ is a square in k. Further, in the case $k = \mathbb{Q}$, this assertion is equivalent with: there exists a positive integer $c \in \mathbb{Z}$ such that $(2a, c, b + 2) \in \mathbb{Q}^3$ lies on the cone $X^2 + Y^2 = Z^2$, i. e. $(2a, c, b + 2)$ is a *Pythagorean triple*, i. e. the integers $2a, c, b + 2$ are sides of the right-angled triangle with $b + 2$ as hypotenuse. If δ is not a square in k, then 2 is the only zero of g in k, $L = k(\sqrt{\delta})$ and $F = (X - 1)^2(X^2 + aX + (b - 2))$. Therefore by Footnote 28 $G_k(f) = \mathbf{Z}_4$ or $\mathbf{D}_4$ according as $(8 - 4b + a^2) \cdot \delta$ is a square in k or not.

In both the examples above the equation $f(x) = 0$ can be solved by extracting square roots twice!

(3) Let $f(X) = X^4 + pX + p \in \mathbb{Q}[X]$. Then f is irreducible over $\mathbb{Q}$ by Schönemann-Eisenstein criterion, see Footnote 45. The cubic resolvent $g = X^3 - 4pX - p^2 \in \mathbb{Z}[X]$ is irreducible if and only if it has no integer roots, or equivalently, $\pm p$ are not zeroes of g. Therefore g is irreducible over Q if and only if $p \neq 3, 5$. Further, $\mathrm{Disc}(f) = \mathrm{Disc}(g) = -p^3(99p - 64) < 0$ and hence $G_{\mathbb{Q}}(f) = \mathfrak{S}_4$ if $p \neq 3, 5$.

If $p = 3$, then $g = (Y + 3)(Y^2 - 3Y - 3)$, -3 is the only rational zero of g, $L = \mathbb{Q}(\sqrt{21})$ and $F = (X^2 + 3X + 3)(X^2 + 3)$ has no real zeroes and hence F does not split over L. Therefore $G_{\mathbb{Q}}(f) = \mathbf{D}_4$.

If $p = 5$, then $g = (Y - 5)(Y^2 + 5Y + 5)$, 5 is the only rational zero of g, $L = \mathbb{Q}(\sqrt{5})$ and $F = (X^2 - 5X - 5)(X^2 - 5)$ splits into linear factors over L. Therefore $G_{\mathbb{Q}}(f) = \mathbf{Z}_4$.

---

[27] Let $f \in k[X]$ be a polynomial of degree ≥ 2 over an arbitrary field k with a zero $a \in k$ and $h := f/(X - a) \in k[X]$. Then $\mathrm{Disc}(f) = h(a)^2 \cdot \mathrm{Disc}(h)$. One can check this equality by using the formula: $\mathrm{Disc}(f) = (-1)^{\binom{n}{2}} a_0^{2n-2} \prod_{j=1}^{n} f'(x_j)$, where $f = a_0(X - x_1) \cdots (X - x_n)$ and $f' = (d/dX)f$ is the derivative of f.

[28] Two quadratic extensions $k(\sqrt{\alpha})$ and $k(\sqrt{\beta})$ of a field k are equal if and only if $\alpha \cdot \beta$ is a square in k.

(4) Let $f := X^4 + X + b \in \mathbb{Z}[X]$ be a biquadratic irreducible polynomial over $\mathbb{Q}$. Then the cubic resolvent g of f is the cubic polynomial $g = Y^3 - 4bY - 1$ which is irreducible over $\mathbb{Q}$, since the only possible zero of g in $\mathbb{Q}$ is ± 1. Further, $\mathrm{Disc}(f) = \mathrm{Disc}(g) = 256 \cdot b^3 - 27$. Therefore the Galois group $\mathrm{G}_{\mathbb{Q}}(f) = \mathfrak{S}_4$ or $\mathfrak{A}_4$. Moreover, $\mathrm{G}_{\mathbb{Q}}(f) = \mathfrak{A}_4$ if and only if $\mathrm{Disc}(f)$ is a square in $\mathbb{Q}$, or equivalently, in $\mathbb{Z}$, since $b \in \mathbb{Z}$, i. e. there exists an integer $c \in \mathbb{Z}$ such that the point $(b,c) \in \mathbb{Z}^2$ lies on the *elliptic curve* $Y^2 = 256X^3 - 27$. Since elliptic curves over $\mathbb{Q}$ have at most finitely many integer solutions[29], it follows that there are at most finitely many integers $b \in \mathbb{Z}$ such that $\mathrm{G}_{\mathbb{Q}}(f) = \mathfrak{A}_4$.

(5) One can use the above results to compute the Galois groups of the following polynomials over $\mathbb{Q}$: $X^4 + X^3 + X^2 + X + 1$, $5X^4 + 4X^3 + 4X + 5$, $X^4 - 3X^3 + 3X^2 - 3X + 1$, $X^4 + 4X^3 + 12X^2 + 24X + 24$, $4X^4 + 48X^3 + 108X^2 + 72X + 9$ and $12X^4 - 15X^3 + 20X^2 - 30X + 60$.

1.D Solvable Equations – Radical Extensions

In this subsection we come to the question whether formulas, similar to the roots of quadratic, cubic, quartic polynomials already given in the mid-sixteenth century (see Footnote 34), exist for the roots of polynomial equations of *arbitrary degree*. This question occupied mathematicians for a long time and was one of the driving forces for further development of mathematics. It was finally answered in the negative by Abel in 1826 and it provided a decisive impetus for the work of Galois.

Let k be a field of characteristic $p \geq 0$. A zero of the pure polynomial $X^n - c \in k[X]$, $c \neq 0$, where $n \in \mathbb{N}^+$ not a multiple of p, in a field extension K of k is called a r a d i c a l over k and is usually denoted by $\sqrt[n]{c}$ or $c^{1/n}$ called an n-th r o o t of c. The field extension $k(x) = k[x]$ is called a s i m p l e r a d i c a l e x t e n s i o n of k. If the polynomial $X^n - c$ is irreducible in $k[X]$, then x is called an i r r e d u c i b l e r a d i c a l o f d e g r e e n over k. In the case $\mathrm{Char}\, k = p > 0$, a zero x of an Artin-Schreier polynomial $X^p - X - c \in k[X]$ is called a r a d i c a l over k and the field extension $k(x) = k[x]$ is called a s i m p l e r a d i c a l e x t e n s i o n of k. If the polynomial $X^p - X - c$ is irreducible over k, i. e. if $x \notin k$ (see 1.C.8), then the radical x is called i r r e d u c i b l e.

We say that a finite field extension $K|k$ is a r a d i c a l e x t e n s i o n if there exists a chain of fields: $k = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m = K$ such that for each $r = 1, \ldots, m$, the field extension K_r of K_{r-1} is a simple radical extension. Since the simple radical extensions are separable, radical extensions are separable. Moreover:

1.D.1 Lemma *The Galois closure*[30] *of a radical extension $K|k$ is again a radical extension.*

Proof: This is immediate from the fact that the Galois closure K' of K over k is the

[29] The famous theorem of C a r l L u d w i g S i e g e l (1896-1981) asserts that: *The number of integral points on a rational nonsingular curve of genus strictly greater than 0 is finite*. In particular, this applies to nonsingular cubic curves, i. e. elliptic curves, but not to the singular cubic, e. g. $Y^2 = X^3$ has infinitely many integer solutions.

[30] For every finite separable $K|k$ there exists a smallest extension K' of K such that $K'|k$ Galois over k. Moreover, such a extension is unique upto an isomorphism over K and hence $K'|k$ is called the G a l o i s c l o s u r e of $K|k$. In fact, if $x \in K$ is a primitive element of Kover k, then the K' is a (minimal) splitting field of the minimal polynomial $\mu_{x,k}$ of x over k.

compositum[31] (in the algebraic closure $\bar{k}$ of k) of the conjugate fields $\sigma(K)$, $\sigma \in \mathrm{Gal}(K'|k)$ which are also radical extensions and the compositum of two radical extensions is also clearly a radical extension. □

The following precise characterisation of solvable equations given in the theorem below was proved by Galois in 1830 in the case of equations without repeated roots over a field of characteristic 0. However, we will give a proof in arbitrary characteristic based on the one in [8, Band 2, § 93, Beispiel 7]. For this reason one needs to modify the definition of a radical extension in an appropriate way so that the proof of the following theorem works for fields of positive characteristic as well. See remarks after the proof of the Theorem 1.D.2.

1.D.2 Theorem (Galois– Great Theorem[32]) *Let k be a field and let $f \in k[X]$ be a polynomial with separable reduction. Then the following statements are equivalent* :

(i) *The Galois group $\mathrm{G}_k(f)$ of f over k is solvable.*

(ii) *There exists a field extension $L|k$ of finite degree such that f splits over L and there exists a chain of fields $k = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m = L$ such that for each $r = 1, \ldots, m$, the field extension K_r of K_{r-1} is a cyclic Galois extension of prime degree.*

(iii) *There exists a Galois field extension $L|k$ of finite degree such that f splits over L and there exists a chain of fields $k = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m = L$ such that for each $r = 1, \ldots, m$, the field extension K_r of K_{r-1} is a (simple) Galois radical extension of prime degree.*

(iv) *There exists a radical extension $L|k$ of finite degree such that f splits over L.*

Proof: We shall prove (ii) $\Longleftrightarrow$ (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i). The equivalence (i) $\Longleftrightarrow$ (ii) is an easy consequence of the Fundamental Theorem of Galois Theory 1.B.11. For instance the implication (i) $\Rightarrow$ (ii) is trivial and for (ii) $\Rightarrow$ (i) note that the Galois group $\mathrm{Gal}(L|k)$ is solvable by (ii) and hence the Galois group $\mathrm{G}_k(f)$ is a homomorphic image of $\mathrm{Gal}(L|k)$.

(iv) $\Rightarrow$ (i) : We may assume that $L|k$ is a Galois extension by 1.D.1 and choose a (minimal) splitting field K of f over k. Then $\mathrm{G}_k(f) = \mathrm{Gal}(K|k) \cong \mathrm{Gal}(L|k)/\mathrm{Gal}(L|K)$ by Theorem 1.B.11, since $K|k$ is normal by (4) in Footnote 15. Therefore it is enough to prove that: *The Galois group of a radical Galois extension $L|k$ is solvable*. We shall prove this assertion by induction on the length m of a chain of fields $k = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m = L$ of simple radical extensions such that $K_{r-1} \subseteq K_r = K_{r-1}[x_r]$, $r = 1, \ldots, m$. Let K_1' be the Galois closure of K_1 in L. Then $K_1' \subsetneq K_2' \subsetneq \cdots \subsetneq K_m' = L$ with $K_r' := K_{r-1}'[K_r] = K_{r-1}'[x_r]$, $r = 2, \ldots, m$, is a chain of simple radical extensions of length $m-1$ from K_1' to L and hence $\mathrm{Gal}(L|K_1')$ is solvable by induction hypothesis. Now, since $\mathrm{Gal}(L|k)/\mathrm{Gal}(L|K_1') \cong \mathrm{Gal}(K_1'|k)$ is also solvable by Examples 1.C.7 and 1.C.8, it follows that $\mathrm{Gal}(L|k)$ is solvable. The assertion (iv) is weaker than (iii).

---

[31] For subfields E and L of some common field Ω, their compositum $E[L]$ or EL is the (unique) smallest subfield of Ω containing both E and L. It is simply the intersection of all subfields which contain the given subfields E and L.

[32] This spectacular research paper on the theory of equations was submitted to and rejected by the French Academy of Sciences in 1830 and it was not published until 1846, fourteen years after his death. The most important thing to say here is that Galois' analysis of solvability by radicals led to the concept of *solvable group* and gave a drastically simpler approach to all of these questions. Namely, once one proves that $\mathfrak{S}_n$ is not solvable for $n \geq 5$, then one immediately concludes that the general equation of degree ≥ 5 is not solvable by radicals and that Lagrange's approach for the quintic must fail.

Now we come to the proof of the most significant implication (i) $\Rightarrow$ (iii) : Let K be the splitting field of f over k and let $n := \#\mathrm{G}_k(f) = \mathrm{Gal}(K|k)$. Let q be the biggest prime factor of n and let L be a (minimal) splitting field of $X^{q!}-1$ and f with $K \subseteq L$. Finally, let $K' \subseteq L$ be the minimal splitting field of $X^{q!}-1$ over k. Then the extensions $K'|k$ and $L|k$ are Galois extensions, since the polynomials $X^{q!}-1$ and f have separable reductions and the Galois group $\mathrm{Gal}(L|K')$ is a subgroup [33] of the Galois group $\mathrm{Gal}(K|k) = \mathrm{G}_k(f)$. Therefore $\mathrm{Gal}(L|K')$ is solvable. It is enough to construct a chain of fields as in (iii) from k to L, in two steps, namely, from k to K' and from K' to L.

Construction of chain of fields from K' to L as in (iii) : Since $\mathrm{Gal}(L|K')$ is solvable and its order divides $\#\mathrm{G}_k(f) = n$, all primes $p_1, \ldots, p_m$ occurring as indices in any solvable chain of subgroups $\{1\} = G_m \subsetneq G_{m-1} \subsetneq \cdots \subsetneq G_0 = \mathrm{Gal}(L|K')$ such that for each $i = 1, \ldots, m$, G_i is normal in G_{i-1} and $p_i = [G_{i-1} : G_i]$ of $\mathrm{Gal}(L|K')$ must be $\leq q$ (by choice of q). Now, since K' contains all s-th roots of unity for all $s \leq q$, from Examples 1.C.6 and 1.C.8, it follows that the chain $L = L^{G_m} \supsetneq L^{G_{m-1}} \supsetneq \cdots \supsetneq L^{\mathrm{Gal}(L|K')} = K'$ of subfields is a required chain as in (iii).

Construction of chain of fields from k to K' as in (iii) : We shall do this construction by induction on q. For inductive step from $q-1$ to q, we may assume that $q \geq 2$ and by induction hypothesis k contains all s-th roots of unity for all $s < q$. Then K' is the splitting field of $X^q - 1$ over k and hence the Galois group $\mathrm{Gal}(K'|k)$ is abelian of an order which divides $\varphi(q)$ by Example 1.B.3. Therefore the construction of chain of fields from k to K' as in (iii) can be carried out as in the above case from K' to L. □

1.D.3 Remark In the proof of the implication (i)⇒(iii) of the Theorem 1.D.2 one realizes that in the case $p = \mathrm{Char}\, k > 0$, there is no non-trivial Artin-Schreier extension as a part of the chains of subfields constructed above as in (iii) if the biggest prime divisor q of $\#\mathrm{G}_k(f)$ is smaller than p, in particular, if $\deg(\mathrm{Red}\, f) < p$. The condition that p is coprime to $\#\mathrm{G}_k(f)$ is not enough. For example, if $k = \mathbb{F}_2$ and if $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ is a chain of field extensions such that $K|k$ is Galois extension and for all $r = 1, \ldots, m$, $K_r|K_{r-1}$ is Galois radical extension of prime degree, but not Artin-Schreier extension, then K does not contain the field L with 8 elements. This follows from the fact that $\mathrm{Gal}(L|k) = \mathbf{Z}_3$ cannot be the Galois group of a radical extension $K_r|K_{r-1}$, since K does not contain primitive 3-rd roots of unity.

1.D.4 Remark To notice the crucial problem in characteristic $p > 0$, observe that the pure equation $g = X^p - a^p = (X-a)^p$ is not separable and hence a cannot lie in any non-trivial Galois extension. The inseparability of g can be explained by the fact that the group $\mathbf{W}_p(k)$ of p-th roots of unity in a field k of characteristic $p > 0$ is the trivial group $\{1\}$.

A polynomial $f \in k[X]$ which has a separable reduction (similarly, the corresponding equation $f(x) = 0$) is called solvable by radicals if f satisfies the equivalent assertions of the above theorem. The solutions of a solvable equation $f(x) = 0$ can hence be determined by only extracting roots (radicals) and using the basic arithmetic operations. Equations of degree ≤ 4 are always solvable by radicals because their Galois groups are subgroups of $\mathfrak{S}_4$ which is solvable and hence are solvable (see Footnote 23). There are explicit formulae[34] for all solutions of equations of degrees ≤ 4. Pure equations $x^n - a$

[33] This follows from the observation: *Let $K|k$ and $K'|k$ be finite field extensions. Suppose that $K|k$ is normal and $L := K'[K]$* (is the smallest subfield of an algebraic closure of k containing both K and K'). *Then the restriction* (which is defined by normality of $K|k$, see (5) in Footnote 15) $\mathrm{Gal}(L|K') \to \mathrm{Gal}(K|k)$ *is an injective group homomorphism.*

[34] The solutions of the quadratic equation $X^2 + bX + c = 0$ (over a field k of characteristic $\neq 2$) are found by the method of completing squares which was conceived around 500 A.D. by the Indian mathematician Shreedharacharya: $x_\pm = \frac{1}{2}(-b \pm \sqrt{D})$

are solvable by radicals (see Example 1.C.7). Reducing mixed equations to pure equations is what we call solvability by radicals. Further, abelian equations are solvable by radicals. – An equation $f(x)=0$ is called an abelian equation[35] over a field k if its Galois group $\mathrm{G}_k(f)$ is abelian. Over finite fields the equations are always abelian and hence solvable by radicals, since in this case its Galois group is cyclic (see Example 1.B.4) and hence solvable. At this point it seemed reasonable to believe that the equations of degree 5 could be solved by similar means, i. e. starting with the coefficients of the equation one should use rational operations together with extraction of square, cubic and fifth roots. However, in spite of much effort[36] by the most prominent mathematicians in the world,

---

where $D=b^2-4c=(x_+-x_-)^2$ is its discriminant. The solutions of the cubic equation $X^3+aX^2+bX+c=0$ (over a field k of characteristic $\neq 2,\neq 3$) were not discovered until the 16-th century. Around 1515 Scipione del Ferro found a solution but did not publish it. In 1535 the solution was rediscovered by Nicolo Fontana, nicknamed Tartaglia, who also kept it a secret until it was published in 1545 by Geronimo Cardano in his famous work "Ars magna". The first step is to reduce the cubic to the form $X^3+pX+q=0$ by means of the substitution $X\mapsto X-\frac{a}{3}$. The discriminant of this cubic equation is $D=-4p^3-27q^2$. For the solution first substitute $X=U+V$ with indeterminates U,V and $u:=\sqrt[3]{\frac{1}{2}(-q+\frac{1}{9}\sqrt{-3D})}$, $v:=\sqrt[3]{\frac{1}{2}(-q-\frac{1}{9}\sqrt{-3D})}$, where one can choose the 3-rd root in u freely, but manipulate the choice of the 3-rd root in v so that $uv=-p/3$. Then $x=u+v$ is the solution of the given cubic equation (called the Cardano's formula); the other solutions are $\varepsilon u+\varepsilon^2 v$ and $\varepsilon^2 u+\varepsilon v$, where ε is a primitive cubic root of unity. Today these formulae are known as Cardano's formulae. Soon after in 1545, the explicit solutions of equations of degree four were found by Ludovico Ferrari, the brilliant assistant of Cardano. These solutions involve nothing more than the rational operations of addition, subtraction, multiplication and division as well as extractions of square and cube roots. In the above solutions Cardano and Ferrari implicitly assumed the existence of roots; this evolved into the existence of complex roots which come in complex conjugate pairs when the coefficients are real numbers. Then the version of the Fundamental Theorem of Algebra asserts that: *Every non-constant polynomial $f\in\mathbb{R}[X]$ factors into linear and quadratic factors with coefficients in* $\mathbb{R}$. The first attempt to prove the Fundamental Theorem of Algebra was due to Jean le Rond d'Alembert (1717-1783) in 1746 using analytic techniques. In 1749 Euler tried a more algebraic method (still somewhat incomplete) using induction on the exponent 2 in $\deg f$. Euler's proof has some major gaps and Lagrange eventually gave a complete proof in 1772 by correcting all the flaws in Euler's arguments. However, in 1799 Gauss pointed out a critical flaw, namely that Lagrange implicitly takes for granted the existence of "imaginary" roots and gave the first essentially complete proof along the lines of d'Alembert's proof. In 1815 Gauss gave another proof of Fundamental Theorem of Algebra using the methods of Lagrange which apply to the general polynomial f_n, see Example 1.C.5 and Footnote 22. These methods are powerful and can be applied to any field. This leads to the language of field extensions and to the following definition: A field k is called algebraically closed if every non-constant polynomial in $k[X]$ splits completely into linear factors over k. Therefore: *The field $\mathbb{C}$ of complex numbers is algebraically closed.* Using Kronecker's impressive method of construction of splitting fields, one proves that: *For any field k there exists a field extension $\bar{k}$ of k which is unique upto a (non-unique) isomorphism such that $\bar{k}$ is algebraic over k and $\bar{k}$ is algebraically closed.* Such a field extension $\bar{k}$ of k is called the algebraic closure of k. Strictly speaking we should say "an algebraic closure" rather than "the algebraic closure".

[35] This definition was given by Kronecker in 1853 in the special case when its Galois group is cyclic and in the more general case it was given by Jordan. Kronecker's interest in abelian equations is related to his amazing conjecture which states that: *The roots of an abelian equation over $\mathbb{Q}$ can be expressed rationally in terms of a root of unity.* This was proved by Weber in 1886 and is now called the Kronecker-Weber Theorem. The modern version of this theorem is stated as: *For a finite Galois extension $K|\mathbb{Q}$ with $K\subseteq\mathbb{C}$, the following statements are equivalent*: (i) $\mathrm{Gal}(K|\mathbb{Q})$ *is abelian.* (ii) *There exists a root of unity $\zeta_n=e^{2\pi i/n}$ such that $K\subseteq\mathbb{Q}(\zeta_n)$.* Proof of the implication (i)⇒(ii) uses ideas from algebraic number theory. See Footnote 29 for more comments on abelian equations.

[36] After the solutions of cubics and quartics by Cardano and Ferrari, many mathematicians such as François Viète (1540-1603), Johann van Waveren Hudde (1628-1704), René Descartes (1596-1650), Ehrenfried Walter von Tschirnhaus (1651-1708), Leonhard Euler (1707-1783) and Étienne Bézout (1730-1783) simplified and improved these solutions and found entirely new solutions. Many of these methods were analyzed by Lagrange in his famous article *Réflexions sur la résolution algébrique des équations* published in 1770-1771. One of Lagrange's main observations is that the auxiliary polynomials and radicals which are used in the solutions of cubics and quartics come from some rational functions of the roots and hence can be explained in terms of the *resolvent polynomials*: as in Footnote 19 we shall use the language of group actions, although Lagrange didn't use this terminology. Fix a rational function $f\in K$ and consider its orbit $\mathrm{G}f=\{f=f_1,f_2,\ldots,f_r\}$ with distinct $f_1=\sigma_1(f),f_2=\sigma_2(f),\ldots,f_r=\sigma_r(f)$ and $\sigma_1,\sigma_2,\ldots,\sigma_r$ in $\mathfrak{S}_n$. Then *the polynomial $\theta(X)=\prod_{i=1}^{r}(X-f_i)\in K^{\mathfrak{S}_n}[X]$ is separable and irreducible* and is called the resolvent polynomial of f. Lagrange essentially proved that: $\#\mathrm{G}_f$ divides $n!=\#\mathfrak{S}_n$, i. e. the index $[\mathfrak{S}_n:\mathrm{G}_f]=n!/\#\mathrm{G}_f$ is an integer (this is a special case of *Lagrange's theorem* in elementary group theory; nowadays it is stated as: *The order of a subgroup H in a finite group G divides the order of G.*) and hence *the cardinality of the orbit $\mathrm{G}f$ of f is the index of the isotropy subgroup G_f of f* (this is a special case of the *orbit-stabilizer theorem* of group actions). To see how Lagrange began to think in terms of resolvent polynomials, consider the polynomial of degree $n!$ defined by $\Theta(X)=\prod_{\sigma\in\mathfrak{S}_n}(X-\sigma f)\in K^{\mathfrak{S}_n}[X]$. Comparing this with $\theta(X)$ note that $\Theta(X)=\theta(X)^{\#\mathrm{G}_f}$. In particular, the degree of the resolvent polynomial θ is the index $[\mathfrak{S}_n:\mathrm{G}_f]$. With this observation Lagrange hoped to solve equations by finding functions of the roots that gave a resolvent of small degree. Although Lagrange's methods work wonderfully for equations of degree ≤ 4, they fail for equations of degree ≥ 5; since finding resolvents of small degree is equivalent to finding subgroups of $\mathfrak{S}_n$ of small index. But for $n\geq 5$ such subgroups are hard to find. Under the Galois correspondence for the general Galois extension $K|K^{\mathfrak{S}_n}$, the intermediate subfield $K^{\mathfrak{S}_n}(f):=K^{\mathrm{G}_f}$ corresponds

no solution was found for over two and a half centuries. The first mathematician to state definitively that no solution existed (by group theoretic methods) was Ruffini.[37] Ruffini's proof was not accepted universally, but it did help to turn the direction of research away[38] from the problem of finding a solution to the problem of showing that in general no such solution exists for an equation of degree ≥ 5. It was in this setting that the young Abel entered the picture. In 1824 Abel[39] proved that the equations of degree ≥ 5 are in general not solvable by radicals.

---

to the isotropy subgroup G_f, i. e. $\mathrm{Gal}(K|K^{\mathfrak{S}_n}(f)) = G_f$ and $K^{\mathfrak{S}_n}(f) = \mathrm{Fix}_{\mathrm{Gal}(K|K^{\mathfrak{S}_n}(f))}K$. This also proves the remarkable Lagrange's Rational Function Theorem (which is mentioned in [7, Appendix 4, page 99] without proof): *Let f and $g \in K$ be two rational functions. Then $G_f \subseteq G_g$ if and only if $K^{\mathfrak{S}_n}(g) \subseteq K^{\mathfrak{S}_n}(f)$.* i. e. *$g$ is a rational function in f with coefficients in $K^{\mathfrak{S}_n}$.* This shows that Lagrange had an implicit understanding of the Galois correspondence for the general Galois extension $K|K^{\mathfrak{S}_n}$. However, Lagrange proved this assertion differently by using the formula: $\psi(X) = \theta(X)\left(\frac{g_1}{X-f_1} + \cdots + \frac{g_r}{X-f_r}\right)$, where $\theta(X)$ is the resolvent of f and $g_i := \sigma_i(g)$, $i = 1,\ldots,r$. This formula is closely related to the so-called Lagrange's interpolation formula. Since $\theta(X) \in K^{\mathfrak{S}_n}[X]$ and is divisible by $X-f_1,\ldots,X-f_r$, it follows that $\psi(X)$ is a polynomial in X and its coefficients are symmetric. i. e. $\psi(X) \in K^{\mathfrak{S}_n}$. Further, since $\theta(X) = (X-f_1)\cdots(X-f_r)$, $\theta'(f) = \theta'(f_1) = \prod_{j=2}^{r}(f_1-f_j)$ and $\psi(f) = \psi(f_1) = g_1\prod_{j=2}^{r}(f_1-f_j)$, it follows that $g = g_1 = \psi(f)/\theta'(f) \in K^{\mathfrak{S}_n}$. Lagrange could see what was important and thereby enabled his successors to sort out the details of what he did.

[37] In 1779 Ruffini published a massive two volume treatise entitled "Teoria Generale delle Equazioni" in which he claims to show that the general equation of the fifth degree cannot be solved by radicals. For many reasons Ruffini's proof was received with skepticism by mathematical community, but an eminent mathematician Cauchy was very appreciative of his work and found his arguments convincing. Ruffini's work also includes advances in the theory of permutations, which were crucial for his proof, and these results were soon generalized by Cauchy. It turns out that there was a significant gap in Ruffini's proofs, but he did show that $\mathfrak{S}_5$ has no subgroup of index 3 or 4 and for $n = 5$ he proved the irreducibility of resolvent polynomials. In 1815 Cauchy generalized Ruffini's result by showing that the index of a subgroup H of $\mathfrak{S}_n$ is either 2 or at least the largest prime $\leq n$. In 1845 Joseph Louis François Bertrand (1822-1900) proved that for $n \geq 5$ either $H = \mathfrak{A}_n$ or $[\mathfrak{S}_n : H] \geq n$, by assuming Bertrand's Postulate which asserts that : *For every natural number $n > 1$, there exists a prime number p such that $n < p < 2n$.* This postulate was proved by Pafnuty Lvovich Chebyshev (1821-1894) in 1850. Finally, in 1879 Kronecker proved this by using simplicity of the *alternating group* $\mathfrak{A}_n$, $n \geq 5$; further he also proved that if $H \subseteq \mathfrak{A}_n$ is a subgroup, then either $H = \mathfrak{A}_n$ or $[\mathfrak{A}_n : H] \geq n$ (For a proof see also [6, Subsection 1.10]).

[38] The works of Euler and Bézout around the middle of the eighteenth century were grounded on the opinion that general equations were solvable by radicals and that finding the solutions of fifth degree equations was only a matter of clever transformations.

[39] Abel was fascinated by the theory of equations and published three articles on this subject, a fourth one appeared among his posthumous work (see item XVIII of volume II of [1]). He was at work on a major new memoir on this theory when he died, tragically, from tuberculosis in 1829 at the age of 27. Abel published his first proof of this theorem at his own expense in 1824 [1, Volume 1, No. 3] and a longer more elaborate version appeared in the first issue of Crelle's journal in 1826 [1, Vol. 1, No. 7]. It is clear that Abel's proof could not have used Galois theory (as Galois was thirteen years old in 1824, see Footnote 22). How then did Abel prove this theorem? Having proved that the general equation of degree ≥ 5 cannot be solved by radicals, the thrust of his later work was to find conditions on special equations which ensure that they are solvable by radicals. Abel realized that Gauss's method for cyclotomic equations could also be applied to the equations which arise from the division of the lemniscate (which is the curve in the plane defined by the polar equation $r^2 = \cos 2\theta$ and by using the cartesian equation $(x^2+y^2)^2 = x^2-y^2$) and in complete analogy with Gauss' results (for example, by inscribing a regular n-gon in the unit circle, it is easy to see that the constructibility of regular n-gon with straightedge and compass is equivalent to dividing the unit circle into n equal arcs by straightedge and compass), he proved that the lemniscate can be divided into 2^n+1 equal parts by straightedge and compass whenever 2^n+1 is a prime number. The n-division points on the lemniscate led to some remarkable polynomials analogous to the cyclotomic polynomials and the Galois theory of these polynomials enables one to understand when exactly the n-division points can be constructed by straightedge and compass. To prove this assertion Abel was led to the study of doubly periodic functions of a complex variable and the theory of complex multiplication. Pushing his investigations further, Abel gave conditions on the roots $x = x_1,\ldots,x_n$ of a separable equation $f(x) = 0$ over a field k, so that it is solvable by radicals, namely: *There are rational functions $\theta_i \in k(X)$, $i = 2,\ldots,n$ such that $x_i = \theta_i(x)$ for all $i = 2,\ldots,n$ and $\theta_i(\theta_j(x)) = \theta_j(\theta_i(x))$ for all $2 \leq i,j \leq n$.* These conditions precisely mean that $K = k(x)$ is the splitting field of f and the Galois group $G_k(f)$ is commutative. More precisely, since $\mu_{x,k}$ divides f, renumbering $x_1,\ldots,x_n$ if necessary, assume that $V(\mu_{x,k}) = \{x_1,\ldots,x_m\}$ with $m \leq n$. Then $G_k(f) = \{\sigma_1,\ldots,\sigma_m\}$, where for $1 \leq j \leq m$, $\sigma_j : k(x) \to k(x)$ are defined by $\sigma_j(x) = x_j = \theta_j(x)$. Further, $(\sigma_i\sigma_j)(x) = \sigma_i(\sigma_j(x)) = \sigma_i(\theta_j(x)) = \theta_j(\sigma_i(x)) = \theta_j(\theta_i(x)) = \theta_i(\theta_j(x)) = \theta_i(\sigma_j(x)) = \sigma_j(\theta_i(x)) = \sigma_j(\sigma_i(x))$ for all $1 \leq i,j \leq m$ (note that the 3-rd and 7-th equalities use the observation: $\sigma(h(x)) = h(\sigma(x))$ for every rational function $h \in k(x) = k[x]$ and every $\sigma \in \mathrm{Aut}(k(x)|k)$) (see also Footnote 4) and hence $G_k(f)$ is commutative. It is because of this result that in 1880 Weber applied the term "abelian" to commutative groups. Abel never published a general criterion for an equation to be solvable by radicals, but in a letter to August Leopold Crelle (1780-1855) (dated October 18, 1828) he wrote: *If every three roots of an irreducible equation of prime degree are related to one another in such a way that one of them may be expressed rationally in terms of the other two, then the equation is solvable by radicals.* Abel gives no indication of how he came to this result or how he proved it! It is remarkable that this statement is almost identical to the one given in 3.2 which was proved by Galois in 1830 but was not published until 1846.

1.D.5 Remark Let $f \in k[X]$ be a separable polynomial over a field k. If one root of f is contained in a radical extension of k, then the equation $f(x) = 0$ is solvable.

1.D.6 Example Let $k \subseteq \mathbb{R}$ be a subfield and let $f \in k[X]$ be an irreducible polynomial of degree 3 which has only real zeroes or, equivalently, the discriminant $\operatorname{Disc} f$ is positive, cf. Proposition 3.5. For example, $X^3 - 6X + 2$, $X^3 - 39X + 65$, $X^3 - 2pX + p$, p is a prime number. Then there is no radical extension $L|k$ such that f splits over L. Otherwise, by Galois' Great Theorem 1.D.2 there is a tower of subfields $F \subseteq F_1 \subseteq \mathbb{R}$ and a prime number q such that $F_1 = F(x)$ with $x^q \in F$, f is irreducible over F and is reducible over F_1. It follows that $q = 3$ and all 3-rd roots of unity belong to the minimal splitting field of f over $F \subseteq \mathbb{R}$, which is a contradiction.

1.D.7 Example (Casus Irreducibilis[40]) The polynomial $f := X^3 - 15X - 4 \in \mathbb{Q}[X]$ has only real zeroes, since its discriminant $\operatorname{Disc} f > 0$; obviously, $x = 4$ is a root and by Cardano's formulae $4 = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$ for appropriate choices of cube roots. Note that $(2+i)^3 = 2 + 11i$ and $(2-i)^3 = 2 - 11i$ and hence the cube roots in the above formula are $2 + i$ and $2 - i$; their sum is 4. Therefore complex numbers appear in the radicals of Cardano's formulae when the discriminant is positive (see Footnote 34). The puzzle is that we are using complex numbers to express the real roots of a real polynomial.

If an irreducible cubic has all real roots then one *cannot* obtain the roots by adjoining radicals of real numbers only; to prove this assertion we have to use Galois theory!

Let $k \subseteq \mathbb{R}$ be a subfield. We say that a field extension $L|k$ is a real radical extension if $L|k$ is a radical extension and $L \subseteq \mathbb{R}$. Further, $x \in \mathbb{R}$ is said to be obtained by real radicals over k if there is a real radical extension $L|k$ such that $x \in L$. In 1891 Hölder proved[41] the following generalised version of the casus irreducibilis:

1.D.8 Theorem (Hölder) *Let $k \subseteq \mathbb{R}$ be a subfield and $f \in k[X]$ be an irreducible polynomial over k with splitting field $K \subseteq \mathbb{R}$. Then the following statements are equivalent*:

(i) *f has a root which is obtained by real radicals over k,* i. e. *there is a real radical extension $L|k$ such that L contains a root of f.*

(ii) *All roots of f are contained in a real radical extension $L|k$ which is obtained by adjoining square roots only.*

(iii) *$K|k$ is a radical extension.*

(iv) *$[K : k]$ is a power of* 2.

Proof: Most of the implications are easy to prove, for instance, (ii) $\Rightarrow$ (i) is trivial, (iii) $\Rightarrow$ (i) follows from $K \subseteq \mathbb{R}$ and (iv) $\Rightarrow$ (ii) and (iii) are easy consequences of the Fundamental Theorem of Galois Theory 1.B.11. Therefore it is enough to prove the implication (i) $\Rightarrow$ (iv): Suppose on the contrary that some root x of f lies in a real radical extension $L|k$ and that $[K : k] = \#\operatorname{Gal}(K|k)$ is not a power of 2. Then choose an odd prime p which divides $\#\operatorname{Gal}(K|k)$ and hence by Cauchy's theorem, there exists $\sigma \in \operatorname{Gal}(K|k)$ of order p. We may further use Theorem 1.C.1 to assume that $\sigma(x) \neq x$, replacing σ by its suitable conjugate as follows: Let $\mathrm{V}(f) = \{x = x_1, \ldots, x_n\}$, $n := \deg f$, be the set of zeroes of f. Since f is irreducible over k, the Galois group $\mathrm{G}_k(f) = \operatorname{Gal}(K|k)$ operates transitively on $\mathrm{V}(f)$ by Theorem 1.C.1 and hence for each $i = 1, \ldots, n$, there exists $\tau_i \in \operatorname{Gal}(K|k)$ such that $\tau_i(x) = x_i$. Now, since $\sigma \neq \mathrm{id}_K$, there exists i such that $\sigma(x_i) \neq x_i$, we may replace σ by the conjugate $\tau_i^{-1}\sigma\tau_i$.

---

[40] Historically, this term was used for the irreducible cubic. One of the first persons to talk about *casus irreducibilis* was Rafael Bombelli (1526-1572) in his book *L'algebra* published in 1572. He was the first to give systematic rules for adding and multiplying complex numbers. For quadratic equations Cardano pretended that complex solutions did not exist. But for cubics with all real roots Cardano's formulae must involve complex numbers and it is impossible to ignore complex numbers in this case.

[41] See [Hölder, O. L.: Über den Casus Irreducibilis bei der Gleichung dritten Grades, *Math. Annalen*, **38** (1891), 307-321.]

Let $F := \mathrm{Fix}_{\mathrm{H}(\sigma)} K$ denotes the fixed field of the subgroup $\mathrm{H}(\sigma)$ of $\mathrm{Gal}(K|k)$ generated by σ. Then by Galois Correspondence 1.B.11, $K|F$ is a Galois extension with $[K:F] = \#\mathrm{Gal}(K|F) = \#\mathrm{H}(\sigma) = p$. Furthermore, since $x \in K \setminus F$ and $[K:F] = p$ is prime, it follows that $K = F(x)$ and hence by the following Lemma 1.D.9, K cannot be contained in a real radical extension of F.

Now, since $x \in L$, where $L|k$ is a real radical extension, it follows that the compositum $F[L]$ is also a real radical extension of F and K is contained in the real radical extension $K = F(x) \subseteq F[L]$ of F which contradicts the previous paragraph. □

1.D.9 Lemma *Let $E|F$ be a Galois extension with $E \subseteq \mathbb{R}$ and let $[E:F] = p$ for some odd prime number p. Then E cannot be contained in a real radical extension of F.*

Proof: We shall first prove that: *Adjoining a real prime radical*[42] *does not change the degree*, i. e. $[E(y):F(y)] = [E:F]$ *for every $y \in \mathbb{R} \setminus F$ with $y^q \in F$, q a prime number.* Consider the diagram of field extensions:

$$\begin{array}{ccc} F(y) & \subsetneq & E(y) \\ \bigcup & & \bigcup \\ F & \subsetneq & E \end{array} .$$

If $y \in E$, then $F(y) = E$, since $y \notin F$ and $[E:F]$ is prime. The polynomial $X^q - y^q \in F[X]$ has no zero in F, since $F \subseteq \mathbb{R}$, $y \notin F$, and hence[43] $\mu_{y,F} = X^q - y^q$ is the minimal polynomial of y over F. Further, $q = [F(y):F] = [E:F] = p$ is an odd prime and since $E = F(y)|F$ is Galois (and hence normal), E is the splitting field of the minimal polynomial $\mu_{y,F} = X^q - y^q$. But, then $(y \neq 0)$ the primitive q-th root of unity $\zeta_q \in E$ which is impossible, since $E \subseteq \mathbb{R}$. This proves that $y \notin E$ and hence $[E(y):E] = q$ and $[E(y):F(y)] = p = [E:F]$.

Now, suppose that $L|F$ is a real radical extension of F i. e. L is obtained by adjoining successive real prime radicals. Then by the assertion proved above, we have $[L[E]:L] = [E:F] = p$, where $L[E]$ is the compositum of L and E. In particular, $L[E] \neq L$ and hence $E \not\subseteq L$. □

1.D.10 Corollary *Let $k \subseteq \mathbb{R}$ be a subfield and let $f \in k[X]$ be an irreducible polynomial over k of degree* $\deg f$ *which is not a power of* 2. *If f splits completely over $\mathbb{R}$, then no root of f can be obtained by real radicals over k.*

For example, for any prime number p, the cubic polynomial $f = X^3 - 2pX + p \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$ by Schönemann-Eisenstein criterion (see Footnote 45) and has three real roots, since $f(0) > 0$ and $f(1) < 0$. It is amusing to find the roots of this cubic by using Cardano's formulae and see where non-real numbers come in!

We note the following striking consequence of the Theorem 1.D.8:

1.D.11 Corollary *Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial over $\mathbb{Q}$ which splits completely over $\mathbb{R}$. Then all roots of f lie in a radical extension of $\mathbb{Q}$ obtained by adjoining square roots. In particular, roots of f are constructible numbers* (see Footnote 9).

We finally end this subsection by stating without proof the following result of Alfred Loewy (1873-1935) which was proved in 1920:

---

[42] If q is a prime number, then any zero of $X^q - a \in k[X]$ is called a prime radical over k.

[43] (Abel-Kronecker) : *Let q be a prime number. Then the polynomial $f = X^q - a \in k[X]$ is irreducible over a field k if and only if a is not a q-th power in k*, i. e. *f has no zero in k.* For a proof of the non-trivial direction, if f is reducible over k, then there exists a field extension $L|k$ of degree $m < q$ such that f has a zero $x \in L$. Then, from $x^q = a$, it follows that $\mathrm{N}_k^L(x)^q = \mathrm{N}_k^L(x^q) = \mathrm{N}_k^L(a) = a^m$ is a q-th power in k and hence a is a q-th power in k, since $\gcd(m,q) = 1$.

Abel proved this result shortly before his death in 1829 in the special case when k contains a primitive q-th root of unity. The general case was proved by Kronecker in 1879. There is a general version of this result due to Alfredo Capelli (1855-1910) : *A polynomial $f = X^n - a \in k[X]$ over a field k is reducible over k if and only if n has a divisor $d > 1$ such that either a is a d-th power in k or n is divisible by 4 and a is of the form $-4b^4$ with $b \in k$.*

1.D.12 Theorem (Loewy) *Let $f \in k[X]$ be an irreducible polynomial over a subfield k of $\mathbb{R}$, of degree $2^m n$, n odd. Then at most 2^m roots of f can be obtained by real radicals over k.*

§ 2 Solvability of the affine group

In this section we deal with group theoretic results which are used in the next Section. We determine transitive solvable subgroups of the permutation group $\mathfrak{S}_p$, where p is a prime number. These transitive subgroups are precisely subgroups of the affine group of the finite field of cardinality p.

First let us recall: For an arbitrary field K, a map $\sigma : K \to K$ is called affine linear if there exist $a, b \in K, a \neq 0$ such that $\sigma(x) = ax + b$ for all $x \in K$; moreover, the pair $(a,b) \in K^\times \times K$ is uniquely determined by σ and hence we shall denote σ by $\sigma_{a,b}$. The set $\mathrm{Aff}(K)$ of all affine linear maps from K into K form a group under composition and is called the affine group of K. In fact, $\sigma_{a,b} \circ \sigma_{a',b'} = \sigma_{aa',ab'+b}$ and $\sigma_{a,b}^{-1} = \sigma_{a^{-1},-a^{-1}b}$ and hence it is a subgroup of the symmetric group $\mathfrak{S}(K)$. A subgroup G of $\mathfrak{S}(K)$ is called an affine subgroup if $G \subseteq \mathrm{Aff}(K)$, i. e. if every element of G is affine linear. With this now we prove the following theorem:

2.1 Theorem *Let p be a prime number. Then the affine group $\mathrm{Aff}(\mathbb{F}_p)$ of the finite field $\mathbb{F}_p$ of cardinality p is solvable.*

Proof: The map $\varphi : \mathrm{Aff}(\mathbb{F}_p) \to \mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\}$ defined by $\varphi(\sigma_{a,b}) = a$ is a surjective group homomorphism with kernel $\mathrm{Ker}\,\varphi = \{\sigma_{1,b} \in \mathrm{Aff}(\mathbb{F}_p) \mid b \in \mathbb{F}_p\}$ which is isomorphic to the additive group $(\mathbb{F}_p, +)$ of the field $\mathbb{F}_p$. Further, the quotient group $\mathrm{Aff}(\mathbb{F}_p)/\mathrm{Ker}\,\varphi$ is isomorphic to the multiplicative group $(\mathbb{F}_p^\times, \cdot)$. In particular, both $\mathrm{Ker}\,\varphi$ and the quotient group $\mathrm{Aff}(\mathbb{F}_p)/\mathrm{Ker}\,\varphi$ are solvable. Therefore $\mathrm{Aff}(\mathbb{F}_p)$ is solvable. □

For a proof of Galois' Theorem 3.1 we need the following important lemma which deals with transitive subgroups of $\mathfrak{S}_p$.

2.2 Lemma *Let p be a prime and let $G \subseteq \mathfrak{S}_p$ be a transitive subgroup. Then*

(1) *Every non-trivial normal subgroup N of G also acts transitively on $\{1, 2, \cdots, p\}$.*
(2) *If G is solvable, then G has a unique subgroup*[44] *H of order p* (which is necessarily normal in G).
(3) *If G has a normal subgroup H of order p, then G is an affine subgroup. In particular, G is solvable.*

[44] This unique subgroup H of order p of G is the (unique) p-Sylow subgroup of G. Therefore G and also every normal subgroup $N \neq \{1\}$ of G is isomorphic to the semi-direct product of the group $\mathbb{Z}_p$ with a (cyclic) subgroup of $(\mathbb{Z}_p)^\times$. Moreover, the map $\mathrm{Aff}(\mathbb{F}_p) \to \mathbb{F}_p \rtimes \mathbb{F}_p^\times$, $\sigma_{a,b} \mapsto (b,a)$ is an isomorphism. (note that we have identified $\mathrm{Aut}(\mathbb{F}_p, +) = \mathbb{F}_p^\times$, with this identification the product on the semidirect product $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$ is given by the formula: $(a,b) \cdot (a',b') = (a + ba', bb')$.) In particular, $\#G = pt$ where t is a divisor of $p-1$. The group G is uniquely determined by its order pt and is also called the Frobenius group usually denoted by F_{pt}. The Frobenius group $\mathrm{F}_{p(p-1)}$ is isomorphic to the affine group $\mathrm{Aff}(\mathbb{F}_p)$.

Proof: (1) The class equation for the natural operation of N on $\mathrm{I}_p := \{1,\dots,p\}$ is

$$p = \#\mathrm{I}_p = \sum_{\mathrm{I}_p\backslash N} \#Na\,,$$

where Na denotes the orbit of $a \in \mathrm{I}_p$ and the sum runs over the quotient set $\mathrm{I}_p\backslash N$. Further, since G is transitive, there exists $\sigma \in G$ such that $\sigma(a) = b$. Therefore, since N is normal in G, we have $Nb = (\sigma N\sigma^{-1})b = \sigma Na$ and hence σ induces a bijection $\sigma : Na \to Nb$. This proves that any two orbits have the same cardinality, namely $\#N > 1$, since N is non-trivial. Further, since p is prime, from $p = \#N \cdot \#\mathrm{I}_p\backslash N$, we get $\#\mathrm{I}_p\backslash N = 1$, i. e. N is transitive.

(2) We may assume that $\#G > p$. Since G is transitive on I_p, we have $\mathrm{I}_p = Ga$ for all $a \in \mathrm{I}_p$ and hence p is the index of isotropy G_a which divides $\#G$. Now, since G is solvable and $\#G > p$, there exists a normal subgroup $N \subsetneq G$, $N \neq \{1\}$. By part (1) N is also transitive on I_p. Therefore, by induction on $\#G$, N has a unique subgroup H of order p. Note that H must be a characteristic subgroup of N, i. e. $\varphi(H) = H$ for every automorphism $\varphi : N \to N$ of N. In particular, H is normal in G, since every inner automorphism of G induces an automorphism of N. It remains to prove the uniqueness of H. Suppose that H' is another subgroup of G of order p. Then $H \cap H' = \{1\}$ and the quotient group $HH'/H \cong H'/(H' \cap H) = H'$ and hence HH' is a subgroup of order p^2. In particular, p^2 divides $\#G$, but $\#G$ divides $p!$ which is a contradiction.

(3) Let H be a normal subgroup of G of order p. Then, since p is prime, H must be cyclic generated by a p-cycle $\tau \in G$. We may assume that $\tau = \{0, 1, \dots, p-1\}$. By identifying $\{1,\dots,p\}$ with $\mathbb{F}_p = \{0,1,\dots,p-1\}$ by $i \longleftrightarrow i-1$, $i = 1,\dots,p$ and using the relation $\equiv_p$ addition modulo p, we may further assume that

$$\tau(x) = x+1 \quad \text{for all} \quad x \in \mathbb{F}_p\,. \tag{2.2.3.1}$$

This shows that G is a subgroup of $\mathfrak{S}(\mathbb{F}_p)$ and τ is translation by 1 which is affine linear. Moreover, since the subgroup $H = \mathrm{H}(\tau)$ is normal in G, for every $\sigma \in G$, $\sigma\tau\sigma^{-1} \in \mathrm{H}(\tau)$, i. e. $\sigma\tau\sigma^{-1} = \tau^a$ for some $a \in \mathrm{I}_p$. Therefore, $\sigma\tau(x) = \tau^a\sigma(x)$ for all $x \in \mathbb{F}_p$ and hence by (2.2.3.1) $\sigma(x+1) = \sigma(x) + a$, i. e. $\sigma(x) = ax + b$ for all $x \in \mathbb{F}_p$, where $b = \sigma(0)$. This proves that G is an affine subgroup of $\mathfrak{S}(\mathbb{F}_p)$. Therefore, since subgroup of a solvable group is solvable, G is solvable by 2.1. □

§3 Solvable Equations of Prime Degree

In this section, as an application of Galois theory, we prove the following theorem of Galois which determines the Galois groups of irreducible equations of prime degree that are solvable.

3.1 Theorem (Galois) *Let $f \in k[X]$ be an irreducible separable polynomial of prime degree p over a field k. If f is solvable by radicals over k, then the Galois group $\mathrm{G}_k(f)$ of f over k is an affine subgroup of the symmetric group $\mathfrak{S}_p$ on p symbols.*

Proof: Since f is separable and irreducible over k, by 1.C.1 the Galois group $\mathrm{G}_k(f)$ operates transitively on the set $\mathrm{V}(f) = \{x_1,\dots,x_p\}$ of the zeroes of f. With this we

identify $\mathrm{G}_k(f)$ with a transitive subgroup of $\mathfrak{S}_p$. Further, $p = \deg f = [k(x_1) : k]$ divides $[k(x_1,\ldots,x_p) : k] = \#\mathrm{G}_k(f)$ and hence by *Cauchy's theorem*, $\mathrm{G}_k(f)$ has an element τ of order p. Then, since p is prime, τ must be a p-cycle. Since f is solvable by radicals, by 1.D.2 $\mathrm{G}_k(f)$ is solvable and hence by 2.2 (2) the subgroup $H = \mathrm{H}(\tau)$ generated by τ must be the unique normal subgroup in $\mathrm{G}_k(f)$ of order p. Therefore by 2.2 (3) $\mathrm{G}_k(f)$ is an affine subgroup of $\mathfrak{S}_p$. □

In order to justify the use of group theory and to demonstrate its power, we now come to some consequences of Theorem 2.1 (proved in Section 2) which do not refer to groups in their statements but for their proofs we make use of group theory. Some results of this nature were already quoted by Galois. For example, the following result is Proposition 8 in his memoir [4, p. 69] (see also [3, p. 113]).

3.2 Theorem (Galois) *Let $f \in k[X]$ be an irreducible separable polynomial of prime degree p over a field k. Then f is solvable by radicals if and only if all zeroes of f can be rationally (over k) expressed from any two zeroes x, y of them,* i. e. *$k(x,y)$ is the splitting field of f over k. Moreover, in this case $\mathrm{G}_k(f)$ is isomorphic to a subgroup of $\mathrm{Aff}(\mathbb{F}_p)$ and there exists an intermediary subfield L of the minimal splitting field $K|k$ of f over k such that*

(1) *$L|k$ is a cyclic Galois extension of degree m which divides $p-1$.*

(2) *Every normal extension $E|k$ with $k \subseteq E \subsetneq K$ is contained in L.*

(3) *The field extension $K|L$ is a cyclic Galois extension of degree p.*

Proof: Since f is separable and irreducible over k, by 1.C.1 the Galois group $\mathrm{G}_k(f)$ operates transitively on the set $\mathrm{V}(f) = \{x_1,\ldots,x_p\}$ of zeroes f. With this we identify $\mathrm{G}_k(f)$ with a transitive subgroup of $\mathfrak{S}_p$.

Suppose that f is solvable by radicals, then $\mathrm{G}_k(f) \subseteq \mathrm{Aff}(\mathbb{F}_p)$ by 3.1. In particular, for arbitrary $x, y \in \mathrm{V}(f)$, $\mathrm{Gal}(K|k(x,y)) \subseteq \mathrm{G}_k(f) \subseteq \mathrm{Aff}(\mathbb{F}_p)$ and so every $\sigma \in \mathrm{Gal}(K|k(x,y))$ is of the form $\sigma(z) = az + b$ for all $z \in \mathbb{F}_p$, $(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p$. But since $\sigma(x) = x$ and $\sigma(y) = y$, it follows that $a = 1$ and $b = 0$, i.e. $\sigma = \mathrm{id}_{\mathbb{F}_p}$. This proves that the Galois group $\mathrm{Gal}(K|k(x,y))$ of the field extension $K|k(x,y)$ is trivial and hence $K = k(x,y)$, since the field extension $K|k(x,y)$ is Galois by the Fundamental Theorem of Galois Theory 1.B.11.

Conversely, suppose that $K = k(x,y)$ for arbitrary $x, y \in \mathrm{V}(f)$. Then $k(x,y)|k$ is a Galois extension with Galois group $\mathrm{G}_k(f)$ and hence $\#\mathrm{G}_k(f) = [k(x,y) : k(x)][k(x) : k]$. Further, since f is irreducible and $f(x) = 0$, $f = \mu_{x,k}$; moreover, $g := f/(X - x) \in k(x)[X]$ and $g(y) = 0$, it follows that $\mu_{y,k(x)}$ divides g in $k(x)[X]$. Therefore p divides $\#\mathrm{G}_k(f)$ and $\#\mathrm{G}_k(f) = \deg \mu_{y,k(x)} \deg \mu_{x,k} \leq p(p-1)$. Now, by Cauchy's theorem there exists an element $\tau \in \mathrm{G}_k(f)$ of order p and hence the subgroup $H := \mathrm{H}(\tau)$ of $\mathrm{G}_k(f)$ generated by τ is of order p. Further, we claim that H is normal in $\mathrm{G}_k(f)$. Assuming the contrary, there exists $\sigma \in \mathrm{G}_k(f)$ such that $\sigma H \sigma^{-1} = H' \neq H$. But then $H \cap H' = \{1\}$ and so $p^2 = \#HH' \leq \#\mathrm{G}_k(f) \leq p(p-1)$ a contradiction. This proves that H is normal in $\mathrm{G}_k(f)$ and hence by 2.2 (3) $\mathrm{G}_k(f)$ is solvable. Therefore f is solvable by radicals.

For the last part take $L := \mathrm{Fix}_H K$, where $H \subseteq \mathrm{G}_k(f)$ is a normal subgroup of order p which exists by 2.2 (2) and use the Fundamental Theorem of Galois Theory. □

Using the above theorem we can easily write examples of non-solvable equations over the field of rational numbers $\mathbb{Q}$. For example:

3.3 Corollary (Kronecker) *Let $f \in k[X]$ be an irreducible polynomial of prime degree p, where k is a subfield of the field $\mathbb{R}$ of real numbers. If f is solvable by radicals (over k), then either all zeroes of f are real, or f has exactly one real zero. In particular, if f has at least two real zeroes but not all zeroes are real, then the equation $f(x) = 0$ is not solvable by radicals.*

The above condition on the zeroes of $f \in \mathbb{Q}[X]$ can be easily checked arithmetically with the help of the discriminant $\operatorname{Disc} f$ of f and the Proposition 3.5 below:

3.4 Corollary *Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p. If f is solvable by radicals, then the discriminant* $\operatorname{Disc} f$ *of f is*

$$\begin{cases} > 0, & \text{if} \quad p \equiv 1 \pmod 4, \\ > 0, & \text{if} \quad p \equiv 3 \pmod 4 \text{ and if all zeroes of } f \text{ are real}, \\ < 0, & \text{if} \quad p \equiv 3 \pmod 4 \text{ and if } f \text{ has exactly one real zero}. \end{cases}$$

3.5 Proposition *Let $f \in \mathbb{R}[X]$ be a monic separable polynomial of degree n. If f has exactly r real zeroes, then $n-r$ is even and moreover, the signature of the discriminant* $\operatorname{Disc} f$ *of f is determined by the integer $(n-r)/2$,* i. e. $\operatorname{Sign}\operatorname{Disc} f = (-1)^{(n-r)/2}$. *Moreover, 4 divides $n-r$ if and only if the discriminant of f is positive.*

Proof: Let $x_1, \ldots, x_r \in \mathbb{R}$ and let $z_1, \overline{z_1}, \ldots, z_s, \overline{z_s} \in \mathbb{C} \setminus \mathbb{R}$ be all (distinct) zeroes of f. Then the discriminant of f is $\operatorname{Disc} f = D_1 D_2 D_3 D_4 D_5$, where

$D_1 := \prod_{1 \le i < j \le r} (x_i - x_j)^2$,

$D_2 := \prod_{\substack{1 \le i \le r \\ 1 \le k \le s}} (x_i - z_k)^2 (x_i - \overline{z_k})^2$,

$D_3 := \prod_{1 \le k \le \ell \le s} (z_k - \overline{z_\ell})^2 (\overline{z_k} - z_\ell)^2$,

$D_4 := \prod_{1 \le k \le \ell \le s} (z_k - z_\ell)^2 (\overline{z_k} - \overline{z_\ell})^2$,

$D_5 := \prod_{1 \le k \le s} (z_k - \overline{z_k})^2$ and hence the signature of $\operatorname{Disc} f$ is determined by D_5 which is the product of squares of $(n-r)/2$ purely imaginary complex numbers. Therefore $\operatorname{Sign}\operatorname{Disc} f = (1)^{(n-r)/2}$. □

It is easy to use the Corollary 3.3 to produce polynomials in $\mathbb{Q}[X]$ which are not solvable by radicals. For example:

3.6 Example Let $p \ge 5$, q be prime numbers and let $a \ge 2$ be an integer. Then the polynomial $f = X^p - aqX - q \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$ by *Schönemann-Eisenstein criterion*[45]. Moreover, we claim that f has exactly three real zeroes. To prove this, first note that $f(x) < 0$ for

[45] *Let $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ be a non-constant polynomial of degree n. If there is a prime number p such that $p \mid a_i, i = 0, 1, \ldots, n-1$ but not a_n and p^2 does not divide a_0, then f is irreducible over* $\mathbb{Q}$. In 1846 Theodor Schönemann (1812-1868) and independently in 1850 Ferdinand Gotthold Max Eisenstein (1823-1852) published this criterion. Although it is often called the Eisenstein criterion, Schönemann's name should be included, since he proved it first. Using this criterion a slick proof of the irreducibility of the cyclotomic polynomial Φ_p was given by Eisenstein.

$x << 0$, $f(-1) = -1 + q(a-1) > 0$, $f(0) = -q < 0$ and finally, $f(x) > 0$ for $x >> 0$. Therefore, by *Intermediate Value Theorem*, f has at least three real zeroes. But $f'(X) = pX^{p-1} - aq$ has exactly two real zeroes and hence, f must have exactly three real zeroes by *Rolle's theorem*. Therefore by 3.3 the equation $f(x) = 0$ cannot be solved by radicals.

3.7 Example Let $p \geq 7$ and let $f = (X^2+1)(X-1)(X-2)\cdots(X-(p-2)) - 1 \in \mathbb{Z}[X]$. Then f is irreducible[46] over $\mathbb{Z}$ and hence over $\mathbb{Q}$. Moreover, f has exactly $p-2$ real zeroes. Therefore there is an element of order p in $\mathrm{G}_{\mathbb{Q}}(f)$ and the complex conjugation belongs to $\mathrm{G}_{\mathbb{Q}}(f)$. With this now it is easy to verify that $\mathrm{G}_{\mathbb{Q}}(f) = \mathfrak{S}_p$. In particular, f is affect-free and is not solvable by radicals over $\mathbb{Q}$.

3.8 Remark We mention here without proofs (see [Schur, I: *Gleichungen ohne affect*, Sitzungsberichte der Preussischen Akademie der Wissenschaften (1930), pp. 443-449.]) some interesting examples of Issai Schur (1875 - 1941).

Let $n \geq 4$, p be a prime number with $n/2 < p < n$ (such a prime number exists by *Bertrand's postulate*, see Footnote 37) and let $g := X(X-2)(X-4)\cdots(X-2p+2) - p - 1$, $h := X(X+2)\cdots(X+2m-2) \in \mathbb{Z}[X]$ with $m = n-p$ and $f = gh + 2p \in \mathbb{Z}[X]$. Then f is irreducible over $\mathbb{Q}$ by Schönemann-Eisenstein criterion and has exactly $n-2$ real zeroes. Further, modulo p, f is separable and has the prime factor $X^p - X - 1$. This shows that p divides $\#\mathrm{G}_{\mathbb{Q}}(f)$ and hence $\mathrm{G}_{\mathbb{Q}}(f) = \mathfrak{S}_n$, i.e. f is affect-free and not solvable by radicals over $\mathbb{Q}$.

For $n \geq 1$, let $\mathrm{E}_n := 1 + X + X^2/2 + \cdots + X^n/n! \in \mathbb{Q}[X]$ be the polynomial obtained by truncating the power series e^X. Then E_n has exactly one real zero if n is odd and no real zero if n is even. Moreover, E_n is irreducible over $\mathbb{Q}$. Further, the Galois group $\mathrm{Gal}_{\mathbb{Q}}(\mathrm{E}_n)$ of E_n over $\mathbb{Q}$ is the alternating group $\mathfrak{A}_n$ if $n \equiv 0 \pmod 4$ and $\mathfrak{S}_n$ otherwise.

3.9 Remark It follows from 1.B.11 and 1.C.6 that for every finite group G, there is a Galois extension $K|k$ with $\mathrm{Gal}(K|k)$ is isomorphic to G. In fact, choose $n \in \mathbb{N}^*$ with $G \subseteq \mathfrak{S}_n$ and take $K := \mathbb{Q}(X_1, \ldots, X_n)$ and $k := K^G$. – Over a finite field K a finite group G can be realized upto isomorphism as a Galois group of a finite extension L of K if and only if G is cyclic (see Example 1.B.4. In explicit examples one is often interested in Galois groups of polynomials over $\mathbb{Q}$. For any finite abelian group G, there exists a Galois extension $K|\mathbb{Q}$ with $\mathrm{Gal}(K|\mathbb{Q}) \cong G$. We have also seen in Examples in Remark 3.8 that the symmetric group $\mathfrak{S}_n$ and the alternating group $\mathfrak{A}_n$ occur as the Galois group of a finite field extension of $\mathbb{Q}$. Therefore the important question: *Which groups can occur as the Galois group of a finite field extension of* $\mathbb{Q}$? This question is known as the Inverse Galois Problem and is still unsolved in spite of being actively studied by many mathematicians.

References

[1] Abel, N.-H. : *Œuvres Complètes,* Two volumes, (L. Sylow and S. Lie editors), Grøndahl and Søn, Christiana, 1881.

[2] Artin, E. : *Galois Theory*, Notre Dame Mathematical Lectures Number 2, University of Notre Dame Press, Notre Dame 1942.

[3] Edwards, H. M. : *Galois Theory*, Graduate Texts in Mathematics **101**, Springer-Verlag, New York, 1984.

[46] If $f = gh$ for some $g, h \in \mathbb{Z}[X]$, then $-1 = f(i) = g(i)h(i)$ and so $g(i), h(i) \in \{\pm 1\}$ and $g(i) + h(i) = 0$ for every $i = 1, \ldots, p-2$. From this it follows that $\max\{\deg g, \deg h\} < p-2$. Now, since $(g+h)(i) = 0$ for all $i = 1, \ldots, p-2$, we must have $g = -h$ and $f = -h^2$, a contradiction.

[4] Galois, É. : *Écrits et mémoires mathématiques d'Évariste Galois*. Edition critique intégrale des ses manuscripts et publications. Edited by Robert Bourgne and J.-P. Azra. Preface by Jean Dieudonné. Paris: Gauthier-Villars and Cie., 1962.

[5] Jacobson, N. : *Lectures in Abstract Algebra*, Volume III, D. Van Nostrand Co., Inc. East-West Press Pvt. Ltd. New Delhi, 1966.

[6] Patil, D. P. ; Storch, U. : *Group Actions and Elementary Number Theory*, to appear in IISc Journal, Vol. **91**, No. 1 ; pp. 01 - 45.

[7] Rotman, J. : *Galois Theory*, Universitext, Springer-Verlag, New York-Berlin-Heidelberg, ^{2}1998.

[8] Scheja, G.; Storch, U.: *Lehrbuch der Algebra*, Teil 1, 2. B. G. Teubner, Stuttgart ^{2}1994, 1988.

[9] Weber, H.: *Lehrbuch der Algebra*, Band I, II, III, Braunschweig ^{2}1898, ^{2}1899, ^{2}1908.

Received 23 December 2010; Revised 19 February 2011

Anshoo Tandon obtained his B.E. degree in Computer Science and Engineering (1998) from Kumaon University, Nainital, and M.E. in Signal Processing (2000) from Indian Institute of Science, Bangalore. Since 2000 he has worked for different organizations on the broad area of implementation of algorithms related to wireless physical layer. He is currently Principal Engineer at Broadcom, Bangalore.

Anirban Ghatak received his B. Tech. degree in Electronics and Communication Engineering from University of Kalyani in 2001 and M. Tech. in Radiophysics and Electronics from Calcutta University in 2003. He is currently a doctoral student at the Indian Institute of Science, Bangalore, in the department of Electrical Communication Engineering. His interests include classical coding theory, MIMO and network coding.