Chapter 13

Ruffini and Abel on General Equations

13.1 Introduction

Lagrange's investigations were primarily aimed at the solution of "general" equations, i.e. equations whose coefficients are letters, such as

$$X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n = 0$$

(see Definition 8.1, p. 98). At about the same time when Gauss completed the solution of the class of particular equations which arise from the division of the circle (known as cyclotomic equations), Lagrange's line of investigation bore new fruits in the hands of Paolo Ruffini (1765–1822). In 1799, Ruffini published a massive two-volume treatise: "Teoria Generale delle Equazioni" [51, t. 1, pp. 1–324], in which he proves that the general equations of degree at least 5 are not solvable by radicals.

Ruffini's proof was received with skepticism by the mathematical community. Indeed, the proof was rather hard to follow through the 516 pages of his books. A few years after the publication, negative comments were made but, to Ruffini's dismay, no clear, focused objection was raised. Vague criticism was denying Ruffini the credit of having validly proved his claim. Negative reactions prompted Ruffini to simplify his proof, and he eventually came up with very clean arguments, but distrust of Ruffini's work did not subside. Typical in this respect is the following anecdote: in order to get a clear, motivated pronouncement from the French Academy of Sciences, Ruffini submitted a paper to the Academy in 1810. A year later, the referees (Lagrange, Lacroix and Legendre) had not yet given their conclusions. Ruffini then wrote to Delambre, who was secretary of the Academy, to withdraw his paper. In his reply, Delambre explains the referees' attitude:

> Whatever decision Your Referees would have reached, they had to work considerably either to motivate their approval or to refute Your proof. You know how precious is time to realize also how reluctant most geometers are to occupy themselves for a long time with the works of each other, and if they would have happened not to be of Your opinion, they would have had to be moved by a quite powerful motive to enter the lists against a geometer so learned and so skillful. [51, t. 3, p. 59].

At least, unconvincing as it was, Ruffini's proof seems to have completed the reversal of the current opinion towards general equations: while the works of Bezout and Euler around the middle of the eighteenth century were grounded on the opinion that general equations were solvable, and that finding the solution of the fifth degree equations was only a matter of clever transformations, the opposite view became common in the beginning of the nineteenth century (see Ayoub [4, p. 274]). Some comments of Gauss may also have been influential in this respect. In his proof of the fundamental theorem of algebra, [23, §9], Gauss writes:

> After the works of many geometers left very little hope of ever arriving at the resolution of the general equation algebraically, it appears more and more likely that this resolution is impossible and contradictory.

He voiced again the same skepticism in Article 359 of "Disquisitiones Arithmeticae."

Ruffini's credit also includes advances in the theory of permutations, which was crucial for his proof. Ruffini's results in this direction were soon generalized by Cauchy. Incidentally, it is noteworthy that Cauchy was very appreciative of Ruffini's work and that he supported Ruffini's claim that his proof was valid (see [51, t. 3, pp. 88–89]). In fact, it now appears that Ruffini's proofs do have a significant gap, which we shall point out below.

In 1824, a new proof was found by Niels-Henrik Abel (1802–1829) [1, n° 3], independently of Ruffini's work. An expanded version of Abel's proof was published in 1826 in the first issue of Crelle's journal (the "Journal für die reine und angewandte Mathematik") [1, n° 7]. This proof also contains some minor flaws (see [1, vol. 2, pp. 292–293]), but it essentially settled the issue of solvability of general equations.

Abel's approach is remarkably methodical. He explains it in some detail in the introduction to a subsequent paper: "Sur la résolution algébrique des équations"

(1828) [1, n° 18].

> To solve these equations [of degree at most 4], a uniform method has been found, and it was believed that it could be applied to equations of arbitrary degree; but in spite of the efforts of a Lagrange and other distinguished geometers, one was not able to reach this goal. This led to the presumption that the algebraic solution of general equations was impossible; but that could not be decided, since the method which was used could not lead to definite conclusions except in the case where the equations were solvable. Indeed, the purpose was to solve equations, without knowing whether this was possible. In this case, one could get the solution, although that was not sure at all; but if unfortunately the solution happened to be impossible, one could have sought it for ever without finding it. In order to obtain unfailingly something in this matter, it is therefore necessary to take another way. One has to cast the problem in such a form that it be always possible to solve, which can be done with any problem. Instead of seeking a relation of which it is not known whether it exists or not, one has to seek whether such a relation is indeed possible. For instance, in the integral calculus, instead of trying by a kind of divination or by trial and error to integrate differential formulas, one has to look rather whether it is possible to integrate them in this or that way. When a problem is thus presented, the statement itself contains the seed of the solution and shows the way that is to be taken; and I think that there will be few cases where one could not reach more or less important propositions, even when one could not completely solve the question because the calculations would be too complicated.

The method which is thus advocated by Abel can be interpreted in the realm of algebraic equations as a kind of generic method. One has to find the most general form of the expected solution and work on it to investigate what kind of information can be obtained on this expression if it is a root of the general equation. Abel thus proves, by an intricate inductive argument, that if an expression by radicals is a root of the general equation of some degree, then every function of which it is composed is a rational expression of the roots (see Theorem 13.13, p. 224, for a precise statement). This fills a gap in Ruffini's proofs. Some delicate arguments involving the number of values of functions under permutations of the variables

and, in particular, a theorem of Cauchy generalizing earlier results of Ruffini, complete the proof. This last part of the proof can be significantly streamlined by using arguments from the last of Ruffini's proofs, as Wantzel later noticed. In the following sections, we shall present this easy version, but we point out that this approach unfortunately downplays the advances in the theory of permutations (i.e. in the study of the symmetric group S_n) which were prompted by Ruffini's earlier work.

13.2 Radical extensions

Abel's calculations with expressions by radicals, which we discuss in this section and the following as a first step in the proof that general equations of degree higher than 4 are not solvable, can be adequately cast into the vocabulary of field extensions. This point of view will be used throughout since it is probably more enlightening for the modern reader.

An expression by radicals is constructed from some quantities which are regarded as known (usually the coefficients of an equation, in this context) by the four usual operations of arithmetic and the extraction of roots. This means that any such expression lies in a field obtained from the field of rational expressions in the known quantities by successive adjunctions of roots of some orders. In fact, it is clearly sufficient to consider roots of prime order, since if $n = p_1 \cdots p_r$ is the factorization of a positive integer n into prime factors, then

$$a^{1/n} = \left(\ldots\left((a^{1/p_1})^{1/p_2}\right)\ldots\right)^{1/p_r}.$$

This shows that an n-th root of any element a can be obtained by extracting a p_1-th root a^{1/p_1} of a, next a p_2-th root of a^{1/p_1} and so on. Moreover, it obviously suffices to extract p-th roots of elements which are not p-th powers, otherwise the base field is not enlarged. We thus come to the notion of a radical field extension. Before spelling out this notion in mathematical terms, we note that, in order to avoid some technical difficulties, we shall restrict attention throughout the chapter to fields of characteristic zero; in other words, we shall assume that $1+1+\cdots+1 \neq 0$ or that every field under consideration contains (an isomorphic copy of) the field $\mathbb{Q}$ of rational numbers. This is of course the classical case, which was the only case considered by Ruffini and Abel.

13.1. DEFINITIONS. A field R containing a field F is called a *radical extension of height* 1 of F if there exist a prime number p, an element $a \in F$ which is not a

p-th power in F and an element $u \in R$ such that

$$R = F(u) \qquad \text{and} \qquad u^p = a.$$

Such an element u is sometimes denoted by $a^{1/p}$ or $\sqrt[p]{a}$, and, accordingly, one sometimes writes

$$R = F(a^{1/p}) \qquad \text{or} \qquad R = F(\sqrt[p]{a}).$$

This is in fact an abuse of notation, since the element u is not uniquely determined by a and p. There are indeed p different p-th roots of a. Worse still, the field R itself is in general not uniquely determined by F, a and p. For instance, there are three subfields of $\mathbb{C}$ which qualify as $\mathbb{Q}(2^{1/3})$. (See however Exercises 4 and 5.) Therefore, the notation above will be used with caution.

Radical extensions of height h, for any positive integer h, are defined inductively as radical extensions of height 1 of radical extensions of height $h-1$. More precisely, a field R containing a field F is called a *radical extension of height* h of F if there is a field R_1 between R and F such that R is a radical extension of height 1 of R_1 and R_1 is a radical extension of height $h-1$ of F. Thus, in this case we can find a tower of extensions between R and F,

$$R \supset R_1 \supset R_2 \supset \cdots \supset R_{h-1} \supset F$$

such that, letting $R = R_0$ and $F = R_h$, we have for $i = 0, \ldots, h-1$

$$R_i = R_{i+1}\big(a_i^{1/p_i}\big)$$

for some prime number p_i and some element $a_i \in R_{i+1}$ which is not a p_i-th power in R_{i+1}.

We simply term *radical extension* any radical extension of some (finite) height and, for completeness, we say that any field is a *radical extension of height* 0 of itself.

The definitions above are quite convenient to translate into mathematically amenable terms questions concerning expressions by radicals. For instance, to say that a complex number z has an expression by radicals means that there is a radical extension of the field $\mathbb{Q}$ of rational numbers containing z. More generally, we shall say that an element v of a field L *has an expression by radicals over some field* F *contained in* L if there is a radical extension of F containing v.

Likewise, we say that a polynomial equation $P(X) = 0$ over some field F is *solvable by radicals over* F if there is a radical extension of F containing a root

of P. In the case of general equations

$$P(X) = (X - X_1)\cdots(X - X_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n = 0,$$

we are concerned with radical expressions involving only the coefficients $s_1, \ldots, s_n$, so the base field F will be the field of rational fractions in $s_1, \ldots, s_n$ (which can be considered as independent indeterminates, according to Remark 8.8(a), p. 105). To be more precise, we have to specify a field of reference in which the rational fractions are allowed to take their coefficients. A logical choice is of course the field $\mathbb{Q}$ of rational numbers, but in fact, since we are aiming at a negative result, the reference field can be chosen arbitrarily large. Indeed, we shall prove that if an equation is solvable by radicals over some field F, then it is solvable by radicals over every field L containing F; therefore, if the general equation of degree n is not solvable over $\mathbb{C}(s_1, \ldots, s_n)$, it is not solvable over $\mathbb{Q}(s_1, \ldots, s_n)$ either.

Of course, Ruffini and Abel did not address in these terms the problem of assigning a reference field, but their free use of roots of unity suggests that all the roots of unity are at their disposal in the base field. The choice $F = \mathbb{C}(s_1, \ldots, s_n)$ seems therefore close in spirit to Ruffini's and Abel's work.

The hypothesis that the base field contains all the roots of unity also has a technical advantage, in that it allows more flexibility in the treatment of radical extensions, as the next result shows:

13.2. PROPOSITION. *Let R be a field containing a field F. If R has the form $R = F(u)$ for some element u such that $u^n \in F$ for some integer n, and if F contains a primitive n-th root of unity (hence all the n-th roots of unity, since the other roots are powers of this one), then R is a radical extension of F.*

In other words, in the definition of radical extensions, we need not require that the exponent n be a prime number, nor that u^n be not the n-th power of an element in F, provided that F contains a primitive n-th root of unity.

Proof. We argue by induction on n. If $n = 1$, then $u \in F$, hence $R = F$ and R is then a radical extension of height 0 of F. We may thus assume that $n \geq 2$ and that the proposition holds when the exponent of u is at most $n - 1$.

If n is not prime, let $n = rs$ for some (positive) integers r, $s < n$. By the induction hypothesis, $F(u)$ is a radical extension of $F(u^r)$ and $F(u^r)$ is a radical extension of F, since u^r satisfies $(u^r)^s \in F$. Therefore, $F(u)$ is a radical extension of F, since it is clear from the definition that the property of being radical is transitive, namely, in a tower of extensions $F \subset K \subset L$, if L is a radical

extension of K and K is a radical extension of F, then L is a radical extension of F.

If n is prime, we consider two cases, according to whether u^n is or is not the n-th power of an element in F. If it is not, then R is a radical extension of F, by definition. If it is, let

$$u^n = b^n$$

for some $b \in F$. If $b = 0$, then $u = 0$ and $R = F$, a radical extension of height 0 of F. If $b \neq 0$, then the preceding equation yields

$$\left(\frac{u}{b}\right)^n = 1,$$

hence u/b is an n-th root of unity. Since the n-th roots of unity are all in F, it follows that $u/b \in F$, hence $u \in F$ and again $R = F$, a radical extension of height 0 of F. □

As an application, we have the following result, which will be useful later through its corollary:

13.3. PROPOSITION. *Let R and L be subfields of a field K, both containing a subfield F. Assume F contains the field $\mathbb{C}$ of complex numbers, so that all the roots of unity are in F. If R is a radical extension of F, then there is a radical extension S of L containing R and contained in K.*

Proof. We argue by induction on the height of R. If this height is zero, then $R = F$ and we can choose $S = L$. We may thus let the height of R be $h \geq 1$ and assume that the proposition holds for radical extensions of height at most $h - 1$. By definition of radical extensions of height h, we can find inside R a radical extension R_1 of F of height $h - 1$ and an element u such that

$$R = R_1(u) \qquad \text{and} \qquad u^p \in R_1$$

for some prime number p. By the induction hypothesis, there is a radical extension S_1 of L in K which contains R_1. Then $u^p \in S_1$ and Proposition 13.2 shows that $S_1(u)$ is a radical extension of L. This extension is contained in K, since $u \in K$ and $S_1 \subset K$, and it contains R, since $R = R_1(u)$ and $R_1 \subset S_1$. It thus satisfies the required conditions. □

13.4. COROLLARY. *Let $v_1, \ldots, v_n$ be elements of a field K containing a field F. Assume that F contains $\mathbb{C}$ and that each of $v_1, \ldots, v_n$ lies in a radical extension*

of F contained in K. Then there is a single radical extension of F in K which contains all of $v_1, \ldots, v_n$.

Proof. We argue by induction on n. There is nothing to prove if $n = 1$, so we may assume that $n \geq 2$ and that the corollary holds for $n - 1$ elements. Hence, there is a radical extension L of F in K which contains $v_1, \ldots, v_{n-1}$. Let R be a radical extension of F in K containing v_n. The preceding proposition shows that there is a radical extension S of L in K containing R. Since S contains both L and R, it contains $v_1, \ldots, v_n$. Since moreover S is a radical extension of L, which is a radical extension of F, it is a radical extension of F. □

So far, we have dealt only with the case where roots of unity are in the base field. In order to reduce more general situations to this case, we have to use Gauss' result that every root of unity has an expression by radicals. Since we now have a formal definition for "expression by radicals," it seems worthwhile to spell out how Gauss' arguments actually fit in this framework.

13.5. PROPOSITION. *For any integer n and any field F, the n-th roots of unity lie in a radical extension of F.*

Proof. It suffices to show that a primitive n-th root of unity ζ lies in a radical extension of F, since the other n-th roots of unity are powers of ζ and lie therefore in the same radical extension as ζ.

We argue by induction on n. For $n = 1$, we have $\zeta = 1$, hence ζ lies in F, which is a radical extension of height 0 of itself. We may thus assume that $n \geq 2$ and that the proposition holds for roots of unity of exponent less than n.

If n is not prime, let $n = rs$ for some (positive) integers r, $s < n$. Then ζ^r is an s-th root of unity. By the induction hypothesis, we can find a radical extension R_1 of F containing ζ^r. By the induction hypothesis again, we can find a radical extension R_2 of R_1 (hence also of F) which contains a primitive r-th root of unity. Then, since $\zeta^r \in R_2$, it follows from Proposition 13.2 that $R_2(\zeta)$ is a radical extension of R_2, hence of F. The proposition is thus proved in this case.

If n is prime, then we have to use Gauss' results. First, we can find a radical extension R_1 of F which contains the $(n-1)$-st roots of unity, by the induction hypothesis. We then consider the Lagrange resolvents $t(\omega)$ as in the proof of Corollary 12.29, p. 195. By Proposition 12.27, p. 193, we have

$$t(\omega)^{n-1} \in R_1$$

for every $(n-1)$-st root of unity ω. Therefore Proposition 13.2 shows that

$R_1(t(\omega))$ is a radical extension of R_1. Adjoining successively all the Lagrange resolvents $t(\omega)$, we find a radical extension R_2 of R_1, whence of F, which contains $t(\omega)$ for all $\omega \in \mu_{n-1}$. From Lagrange's formula (p. 138) it follows that ζ can be rationally calculated from the Lagrange resolvents, hence $\zeta \in R_2$ and the proof is complete. □

We now aim to prove the afore-mentioned fact that solvability of an equation by radicals over some field F implies solvability by radicals over any larger field L. This fact may seem obvious, since every expression by radicals involving elements of F is an expression by radicals involving elements of L. However, it needs a careful justification. The point is that, in building radical extensions or expressions by radicals, we allow only extractions of p-th roots of elements which are not p-th powers in F, but these elements could become p-th powers in the larger field L.

13.6. LEMMA. *Let L be a field containing a field F. For any radical extension R of F, there is a radical extension S of L such that R can be identified to a subfield of S.*

Proof. We argue by induction on the height h of R. If $h = 0$, then $R = F$ and we can choose $S = L$.

If $h = 1$, let $R = F(u)$ where u is such that $u^p = a$ for some element $a \in F$ which is not a p-th power in F. Let also K be a field containing L and over which the polynomial $X^p - a$ splits into a product of linear factors. (The existence of such a field K follows from Girard's theorem (Theorem 9.3, p. 116).) Since u is one of the roots of $X^p - a$, it can be identified with an element in K, and every rational fraction in u with coefficients in F, i.e. every element in R, is then identified with an element in K. We may thus henceforth assume that R is contained in K.

If a is not a p-th power in L, then $L(u)$ is a radical extension of height 1 of L, and this extension contains R since it contains F and u. It thus fulfills the required conditions.

If a is a p-th power in L, then let $b \in L$ be a p-th root of a,

$$b^p = a.$$

Since the p-th powers of u and b are equal, it follows that

$$\left(\frac{u}{b}\right)^p = 1.$$

Therefore, u/b is a p-th root of unity, and Proposition 13.5 shows that there is a radical extension S of L which contains u/b. Since $b \in L$, it follows that $u \in S$, hence $R \subset S$ and the proof is complete in the case where the height h of R is 1.

If $h \geq 2$, the lemma readily follows from the preceding case and the induction hypothesis. Indeed, we can find in R a subfield R_1 which is a radical extension of height $h-1$ of F and such that R is a radical extension of height 1 of R_1. By the induction hypothesis, we may assume that R_1 is contained in a radical extension S_1 of L and, by the case $h = 1$ already considered, R can be identified to a subfield of a radical extension S of S_1. The field S is then a radical extension of L and it satisfies the condition of the lemma. □

13.7. THEOREM. *Let P be a polynomial with coefficients in a field F. If $P(X) = 0$ is solvable by radicals over F, then it is solvable by radicals over every field L containing F.*

Proof. Let R be a radical extension of F containing a root r of P. The preceding lemma shows that we may assume R is contained in some radical extension S of L. The radical extension S then contains the root r, hence $P(X) = 0$ is solvable by radicals over L. □

The following special case of the theorem is particularly relevant for this chapter:

13.8. COROLLARY. *If the general equation of degree n*

$$P(X) = (X - x_1) \cdots (X - x_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n = 0$$

is not solvable by radicals over $\mathbb{C}(s_1, \ldots, s_n)$, then it is not solvable by radicals over $\mathbb{Q}(s_1, \ldots, s_n)$ either.

We may thus henceforth assume that the base field contains all the roots of unity.

13.3 Abel's theorem on natural irrationalities

Any proof that the general equation of some degree is not solvable by radicals obviously proceeds *ad absurdum*. Thus, we assume by way of contradiction that there is a radical extension R of $\mathbb{C}(s_1, \ldots, s_n)$ which contains a root x_i of the

general equation

$$(X - x_1) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n = 0.$$

The first step in Abel's proof (which was missing in Ruffini's proofs) is to show that R can be supposed to lie inside $\mathbb{C}(x_1, \ldots, x_n)$. This means that the irrationalities which occur in an expression by radicals for a root of the general equation of degree n can be chosen to be *natural*, as opposed to *accessory* irrationalities, which designate the elements of extensions of $\mathbb{C}(s_1, \ldots, s_n)$ outside $\mathbb{C}(x_1, \ldots, x_n)$ (see Ayoub [4, p. 268]). (The terms "natural" and "accessory" irrationalities were coined by Kronecker.)

The aim of this section is to prove this result, following Abel's approach in [1, n° 7, §2].

13.9. LEMMA. *Let p be a prime number and let a be an element of some field F, which is not a p-th power in F.*

(a) For $k = 1, \ldots, p-1$, the k-th power a^k is not a p-th power in F either.
(b) The polynomial $X^p - a$ is irreducible over F.

Proof. (a) If k is an integer between 1 and $p-1$, then it is relatively prime to p, whence by Theorem 7.8 (p. 86) we can find integers ℓ and q such that $pq + k\ell = 1$. Then

$$a = (a^q)^p (a^k)^\ell.$$

Therefore, if $a^k = b^p$ for some $b \in F$, then we have

$$a = (a^q b^\ell)^p,$$

in contradiction with the hypothesis that a is not a p-th power in F. This contradiction proves *(a)*.

(b) Let P and Q be polynomials in $F[X]$ such that

$$X^p - a = PQ.$$

We may assume that P and Q are monic, and we have to prove that P or Q is the constant polynomial 1. Let K be an extension of F over which $X^p - a$ splits into a product of linear factors. (The existence of such a field follows from Girard's theorem (Theorem 9.3, p. 116).) Since the roots of $X^p - a$ are the p-th roots of a,

which are obtained from any of them by multiplication by the various p-th roots of unity (see §7.3), we have in $K[X]$

$$\prod_{\omega \in \mu_p} (X - \omega u) = PQ$$

where $u \in K$ is one of the p-th roots of a in K. This equation shows that P and Q split in $K[X]$ into products of factors $X - \omega u$. More precisely, μ_p decomposes into a union of disjoint subsets I and J such that

$$P = \prod_{\omega \in I} (X - \omega u) \qquad \text{and} \qquad Q = \prod_{\omega \in J} (X - \omega u).$$

Consider then the constant term of P, which we denote by b. The above factorization of P shows that

$$b = \Big(\prod_{\omega \in I} \omega\Big)(-u)^k$$

where k denotes the number of elements of I. Since $\omega^p = 1$ for any $\omega \in I$, we get by raising both sides of the preceding equality to the p-th power

$$\big((-1)^k b\big)^p = a^k.$$

Part *(a)* of the lemma then shows that $k = 0$ or $k = p$. In the first case $P = 1$ and in the second $P = X^p - a$, whence $Q = 1$. □

Let now R be a radical extension of height 1 of some field F. By definition, this means that there exists an element $u \in R$ such that $R = F(u)$ and $u^p = a$ for some element $a \in F$ which is not a p-th power in F. Using the preceding lemma, we can give a standard form to the elements of R.

13.10. COROLLARY. *Every element $v \in R$ can be written in a unique way as*

$$v = v_0 + v_1 u + v_2 u^2 + \cdots + v_{p-1} u^{p-1},$$

for some elements $v_0, v_1, \ldots, v_{p-1} \in F$.

Proof. This readily follows from Proposition 12.15 (p. 179), by the preceding lemma. □

In fact, when $v \in R$ is given beforehand outside F, then the element u can be chosen in such a way that $v_1 = 1$ in the expression above, as we now show:

13.11. LEMMA. *Let R be a radical extension of height 1 of some field F and let $v \in R$. If $v \notin F$, then the element $u \in R$ such that $R = F(u)$ and $u^p \in R$ can be chosen in such a way that*

$$v = v_0 + u + v_2 u^2 + \cdots + v_{p-1} u^{p-1}$$

for some $v_0, v_1, \ldots, v_{p-1} \in F$.

Proof. Let u' be an element of R such that $R = F(u')$ and $u'^p = a'$ for some element $a' \in F$ which is not a p-th power in F. By Corollary 13.10, we may write

$$v = v'_0 + v'_1 u' + v'_2 u'^2 + \cdots + v'_{p-1} u'^{p-1}$$

for some $v'_0, \ldots, v'_{p-1} \in F$. These elements are not all zero since $v \notin F$. Let k be an index between 1 and $p-1$ such that $v'_k \neq 0$, and let

$$u = v'_k u'^k. \tag{13.1}$$

Raising both sides of this equation to the p-th power, we get

$$u^p = v'^p_k a'^k.$$

This shows that u satisfies the equation $u^p = a$ with $a = v'^p_k a'^k \in F$.

If a is the p-th power of an element in F, then the last equation shows that a'^k also is a p-th power in F. But then it follows from Lemma 13.9(a) that a' itself is a p-th power in F, which contradicts the hypothesis on u'. Therefore, a is not a p-th power in F.

Since $u \in R$, we obviously have $F(u) \subset R$. In order to prove that $R = F(u)$, it thus suffices to show that every element in R has a rational expression in u with coefficients in F. We first show that the powers of u' have such expressions. For any $i = 0, \ldots, p-1$, we get by raising both sides of equation (13.1) to the i-th power

$$u^i = v'^i_k u'^{ki}. \tag{13.2}$$

Now, recall the permutation σ_k of $\{0, 1, \ldots, p-1\}$ which maps every integer i between 0 and $p-1$ to the unique integer $\sigma_k(i)$ between 0 and $p-1$ such that

$$\sigma_k(i) \equiv ik \mod p$$

(see Proposition 10.6, p. 147). By definition of $\sigma_k(i)$, there is an integer m such that

$$ik - \sigma_k(i) = pm,$$

hence

$$u'^{ik} = (u'^{p})^{m} u'^{\sigma_k(i)}.$$

Therefore, recalling that $u'^{p} = a'$ and letting $b_i = (v_k'^{i} a'^{m})^{-1}$ for $i = 0, \ldots, p-1$, we get from equation (13.2)

$$b_i u^i = u'^{\sigma_k(i)}$$

for $i = 0, \ldots, p-1$. Now, every $x \in R$ has an expression

$$x = \sum_{i=0}^{p-1} x_i u'^{i},$$

with $x_i \in F$ for $i = 0, \ldots, p-1$, which can be alternatively written as

$$x = \sum_{i=0}^{p-1} x_{\sigma_k(i)} u'^{\sigma_k(i)},$$

as σ_k is a permutation of $\{0, \ldots, p-1\}$. Substituting $b_i u^i$ for $u'^{\sigma_k(i)}$, we obtain

$$x = \sum_{i=0}^{p-1} x_{\sigma_k(i)} b_i u^i.$$

This shows that every element in R has a rational expression in u with coefficients in F, whence $R = F(u)$. For the given $v \in R$, the coefficient of u in this expression is 1, since taking $i = 1$ in the calculations above, we find $\sigma_k(1) = k$ and $m = 0$, whence $b_1 = v_k'^{-1}$. This completes the proof. □

13.12. LEMMA. *We keep the same notation as in Lemma 13.11 and assume moreover that F contains a primitive p-th root of unity ζ (whence all the p-th roots of unity, since the others are powers of ζ). If v is a root of an equation with coefficients in F, then R contains p roots of this equation, and u, v_0, v_2, $\ldots$, v_{p-1} are rational expressions of these roots with coefficients in $\mathbb{Q}(\zeta)$.*

Proof. Let $P \in F[X]$ be such that $P(v) = 0$. Using the expression of v as in Lemma 13.11, we derive from P another polynomial Q with coefficients in F,

$$Q(Y) = P(v_0 + Y + v_2 Y^2 + \cdots + v_{p-1} Y^{p-1}) \in F[Y].$$

This definition is designed so that the equation $P(v) = 0$ yields $Q(u) = 0$. On the other hand, u is also a root of the polynomial $Y^p - a$, which is irreducible by Lemma 13.9(b). Therefore, Lemma 12.14 (p. 178) shows that $Y^p - a$ divides

$Q(Y)$, and it follows that every root of $Y^p - a$ is a root of $Q(Y)$. Since the roots of $Y^p - a$ are the p-th roots of a, which are of the form $\zeta^i u$, for $i = 0, \ldots, p-1$, we have

$$Q(\zeta^i u) = 0 \qquad \text{for } i = 0, \ldots, p-1. \tag{13.3}$$

Let then

$$z_i = v_0 + \zeta^i u + v_2 \zeta^{2i} u^2 + \cdots + v_{p-1} \zeta^{(p-1)i} u^{p-1}$$

for $i = 0, \ldots, p-1$. Equation (13.3) yields

$$P(z_i) = 0 \qquad \text{for } i = 0, \ldots, p-1,$$

which proves that R contains p roots of P. To complete the proof, we now show that $u, v_0, v_2, \ldots, v_{p-1}$ are rational expressions of $z_0, \ldots, z_{p-1}$, by calculations which are reminiscent of Lagrange's formula (p. 138). Grouping the terms which contain a given factor $v_j u^j$ in the sum of $\zeta^{-ik} z_i$, we have

$$\sum_{i=0}^{p-1} \zeta^{-ik} z_i = \sum_{j=0}^{p-1} \Big(\sum_{i=0}^{p-1} \zeta^{(j-k)i} \Big) v_j u^j \qquad \text{for } k = 0, \ldots, p-1, \tag{13.4}$$

where we have let $v_1 = 1$. If $j \neq k$, then ζ^{j-k} is a p-th root of unity other than 1, whence a root of

$$\Phi_p(X) = \sum_{i=0}^{p-1} X^i.$$

Therefore,

$$\sum_{i=0}^{p-1} \zeta^{(j-k)i} = 0.$$

Hence, all the terms with index $j \neq k$ vanish in the right-hand side of (13.4), and it remains

$$\sum_{i=0}^{p-1} \zeta^{-ik} z_i = p v_k u^k \qquad \text{for } k = 0, \ldots, p-1.$$

This proves that $v_k u^k$ is a rational expression (indeed a linear expression) of $z_0, \ldots, z_{p-1}$ with coefficients in $\mathbb{Q}(\zeta_p)$. In particular, for $k = 1$, we see that u is such an expression, and since $v_k = (v_k u^k) u^{-k}$, it follows that $v_0, v_2, \ldots, v_{p-1}$ also are rational expressions of $z_0, \ldots, z_{p-1}$ with coefficients in $\mathbb{Q}(\zeta_p)$. □

Now, we let

$$K = \mathbb{C}(x_1, \ldots, x_n),$$

where $x_1, \ldots, x_n$ are independent indeterminates over $\mathbb{C}$, and we denote by F the subfield of symmetric fractions. By Theorem 8.3 (p. 99), we have

$$F = \mathbb{C}(s_1, \ldots, s_n),$$

where $s_1, \ldots, s_n$ are the elementary symmetric polynomials in $x_1, \ldots, x_n$.

13.13. THEOREM (OF NATURAL IRRATIONALITIES). *If an element $v \in K$ lies in a radical extension of F, then there is inside K a radical extension of F containing v.*

Proof. We argue by induction on the height of the radical extension R of F containing v, which is assumed to exist. There is nothing to prove if the height of R is 0 (i.e. if $R = F$) since in this case R lies inside K. We may thus assume the height of R is $h \geq 1$ and consider R as a radical extension of height 1 of some subfield R_1, which is a radical extension of F of height $h - 1$.

If $v \in R_1$, then we are done by the induction hypothesis. For the rest of the proof, we may thus assume that v lies outside R_1. Lemma 13.11 then shows that

$$R = R_1(u)$$

for some element u such that $u^p \in R_1$ (for some prime p) and

$$v = v_0 + u + v_2 u^2 + \cdots + v_{p-1} u^{p-1} \tag{13.5}$$

for some elements $v_0, v_2, \ldots, v_{p-1} \in R_1$. Now, Proposition 10.1 (p. 131) (and its proof) show that every element in K is a root of a polynomial with coefficients in F, which splits into a product of linear factors over K (its roots are the various "values" of the element under the permutations of $x_1, \ldots, x_n$). In particular, v is a root of an equation with coefficients in F (whence in R_1), whose roots all lie in K. Therefore, we can apply Lemma 13.12 to conclude that $u, v_0, v_2, \ldots, v_{p-1} \in K$.

But $u^p, v_0, v_2, \ldots, v_{p-1}$ also lie in R_1, which is a radical extension of height $h - 1$ of F. By the induction hypothesis, $u^p, v_0, v_2, \ldots, v_{p-1}$ all lie in radical extensions of F inside K and, by Corollary 13.4, p. 215, we can find a single radical extension R' of F inside K containing $u^p, v_0, v_2, \ldots, v_{p-1}$. Since $u^p \in R'$, the field $R'(u)$ is a radical extension of R', hence a radical extension of F.

Since moreover we have already observed that $u \in K$, we have $R'(u) \subset K$, and equation (13.5) shows that $v \in R'(u)$. This completes the proof. □

13.4 Proof of the unsolvability of general equations of degree higher than 4

In order to prove that general equations of degree higher than 4 are not solvable by radicals, we have to show, according to Definitions 13.1 above, that for $n \geq 5$ there is no radical extension of $\mathbb{C}(s_1, \ldots, s_n)$ containing a root x_i of the general equation of degree n

$$(X - x_1) \cdots (X - x_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n = 0.$$

The proof we give below is based upon Ruffini's last proof (1813) [51, vol. 2, pp. 162–170]. It is sometimes called the Wantzel modification of Abel's proof (see [51, vol. 2, p. 505] and Serret [53, n° 516]), although Wantzel was relying on Ruffini's papers (see Ayoub [4, p. 270]).

13.14. LEMMA. *Let u and a be elements of $\mathbb{C}(x_1, \ldots, x_n)$ such that*

$$u^p = a$$

for some prime number p, and assume $n \geq 5$. If a is invariant under the permutations

$$\sigma\colon\ x_1 \mapsto x_2 \mapsto x_3 \mapsto x_1; \quad x_i \mapsto x_i \quad \text{for } i > 3$$

and

$$\tau\colon\ x_3 \mapsto x_4 \mapsto x_5 \mapsto x_3; \quad x_i \mapsto x_i \quad \text{for } i = 1, 2 \text{ and } i > 5,$$

then so is u.

Proof. Applying σ to both sides of the equation $u^p = a$, we get $\sigma(u)^p = a$, hence

$$\sigma(u)^p = u^p.$$

Since the lemma is trivial if $u = 0$, we may assume $u \neq 0$ and divide both sides of the preceding equation by u^p. We thus obtain

$$\left(\frac{\sigma(u)}{u}\right)^p = 1,$$

whence

$$\sigma(u) = \omega_\sigma u$$

for some p-th root of unity ω_σ. Applying σ to both sides of this last equation, we get $\sigma^2(u) = \omega_\sigma^2 u$, next $\sigma^3(u) = \omega_\sigma^3 u$. Since σ^3 is the identity map, we have $\sigma^3(u) = u$, whence

$$\omega_\sigma^3 = 1. \tag{13.6}$$

Arguing similarly with τ instead of σ, we find

$$\tau(u) = \omega_\tau u$$

with

$$\omega_\tau^3 = 1. \tag{13.7}$$

From these equations, we also deduce

$$\sigma \circ \tau(u) = \omega_\sigma \omega_\tau u \qquad \text{and} \qquad \sigma^2 \circ \tau(u) = \omega_\sigma^2 \omega_\tau u.$$

However, since

$$\sigma \circ \tau\colon\ x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto x_5 \mapsto x_1; \quad x_i \mapsto x_i \quad \text{for } i > 5$$

and

$$\sigma^2 \circ \tau\colon\ x_1 \mapsto x_3 \mapsto x_4 \mapsto x_5 \mapsto x_2 \mapsto x_1; \quad x_i \mapsto x_i \quad \text{for } i > 5,$$

we have $(\sigma \circ \tau)^5 = (\sigma^2 \circ \tau)^5 = \mathrm{Id}$ (the identity map), whence the arguments above yield

$$(\omega_\sigma \omega_\tau)^5 = (\omega_\sigma^2 \omega_\tau)^5 = 1. \tag{13.8}$$

Since

$$\omega_\sigma = \omega_\sigma^6 (\omega_\sigma \omega_\tau)^5 (\omega_\sigma^2 \omega_\tau)^{-5},$$

equations (13.6) and (13.8) yield

$$\omega_\sigma = 1.$$

From (13.8), we then deduce $\omega_\tau^5 = 1$, and since

$$\omega_\tau = \omega_\tau^6 \omega_\tau^{-5},$$

it follows from equation (13.7) that $\omega_\tau = 1$. This shows that u is invariant under σ and τ. □

13.15. COROLLARY. *Let R be a radical extension of $\mathbb{C}(s_1, \ldots, s_n)$ contained in $\mathbb{C}(x_1, \ldots, x_n)$. If $n \geq 5$, then every element of R is invariant under the permutations σ and τ of Lemma 13.14.*

Proof. We argue by induction on the height of R, which we denote by h. If $h = 0$, then $R = \mathbb{C}(s_1, \ldots, s_n)$ and the corollary is obvious. If $h \geq 1$, then there is an element $u \in R$ and a radical extension R_1 of height $h - 1$ of $\mathbb{C}(s_1, \ldots, s_n)$ such that

$$R = R_1(u) \qquad \text{and} \qquad u^p \in R_1$$

for some prime number p. By induction, we may assume that every element of R_1 is invariant under σ and τ. The lemma then shows that u is also invariant under σ and τ, and, since the elements in R are rational expressions of u, it readily follows that every element in R is invariant under σ and τ. □

We thus reach the conclusion:

13.16. THEOREM. *If $n \geq 5$, the general equation of degree n*

$$P(X) = (X - x_1) \cdots (X - x_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n = 0$$

is not solvable by radicals over $\mathbb{Q}(s_1, \ldots, s_n)$, nor over $\mathbb{C}(s_1, \ldots, s_n)$.

Proof. According to Corollary 13.8, it suffices to show that $P(X) = 0$ is not solvable by radicals over $\mathbb{C}(s_1, \ldots, s_n)$. Assume on the contrary that there is a radical extension R of $\mathbb{C}(s_1, \ldots, s_n)$ containing a root x_i of P. Changing the numbering of $x_1, \ldots, x_n$ if necessary, we may assume that $i = 1$. Moreover, by the theorem of natural irrationalities (Theorem 13.13), this radical extension R may be assumed to lie within $\mathbb{C}(x_1, \ldots, x_n)$. Then, Corollary 13.15 shows that every element of R is invariant under σ and τ. But $x_1 \in R$ and x_1 is not invariant under σ. This is a contradiction. □

Exercises

1. Show that over $\mathbb{R}$ and over $\mathbb{C}$, every equation of any degree is solvable by radicals.

2. Show that the general cubic equation

$$(X - x_1)(X - x_2)(X - x_3) = X^3 - s_1X^2 + s_2X - s_3 = 0$$

is solvable by radicals over $\mathbb{Q}(s_1, s_2, s_3)$. Construct explicitly a radical extension of $\mathbb{Q}(s_1, s_2, s_3)$ containing one of the roots of this cubic and show that this radical extension is not contained in $\mathbb{Q}(x_1, x_2, x_3)$. Thus, the solution of the general cubic equation by radicals over $\mathbb{Q}(s_1, s_2, s_3)$ involves accessory irrationalities.

Same questions for the general equation of degree four.

3. Let ζ_7 (resp. ζ_3) be a primitive 7-th (resp. cube) root of unity. Show that $\mathbb{Q}(\zeta_7)$ is not a radical extension of $\mathbb{Q}$, but that $\mathbb{Q}(\zeta_7, \zeta_3)$ is a radical extension of $\mathbb{Q}$.

4. Let R be a radical extension of a field F, of the form $R = F(a^{1/p})$, for some $a \in F$ which is not a p-th power in F. Find an isomorphism which is the identity on F

$$F[X]/(X^p - a) \xrightarrow{\sim} R.$$

Conclude that all the fields of the form $F(a^{1/p})$ are isomorphic, under isomorphisms leaving F invariant.

5. Show that there are three different subfields of $\mathbb{C}$ of the form $\mathbb{Q}(2^{1/3})$. Show that if F is a subfield of $\mathbb{C}$ containing a primitive p-th root of unity, then for any $a \in F$ which is not a p-th power in F there is only one subfield of $\mathbb{C}$ of the form $F(a^{1/p})$.

6. *To make up partially for the lack of details on the early stages of the theory of groups in Ruffini's and Cauchy's works, the following exercise presents a result of Cauchy on the number of values of rational fractions under permutations of the indeterminates, which was used in Abel's proof that general equations are not solvable by radicals.*

Let n be an integer, $n \geq 3$, let $\Delta = \Delta(x_1, \ldots, x_n)$ be the polynomial defined in §8.3 and let $I(\Delta) \subset S_n$ be the isotropy group of Δ, i.e.

$$I(\Delta) = \{\sigma \in S_n \mid \sigma(\Delta) = \Delta\}.$$

(This subgroup of S_n is called the *alternating group* on $\{1, \ldots, n\}$, and denoted A_n.)

(a) Show that any permutation of n elements is a composition of permutations which interchange two elements and leave the other elements invariant. (Permutations of this type are called *transpositions*.)

(b) Show that a permutation leaves Δ invariant if and only if it is a composition of an even number of transpositions.

(c) Let p be an odd prime, $p \leq n$. Show that the cyclic permutations of length p

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_p \mapsto i_1$$

(where $i_1, \ldots, i_p \in \{1, \ldots, n\}$) generate $I(\Delta)$.
[Hint: By (b), it suffices to show that the composition of any two transpositions is a composition of cycles of length p.]

(d) Let again p be an odd prime, $p \leq n$, and let V be a rational fraction in $x_1, \ldots, x_n$ which takes strictly less than p values under the permutations of $x_1, \ldots, x_n$. Show that V has the form $V = R + \Delta S$ where R and S are symmetric rational fractions, hence that the number of values of V is 1 or 2.
[Hint: Show that V is invariant under the cyclic permutations of length p.]

(e) Translate the result above in the following purely group-theoretical terms: if $G \subset S_p$ is a subgroup of index $< p$ (with p prime), then G contains the alternating group A_p.
[Hint: Use Proposition 10.5, p. 146.]