CHAPTER 5

Fields

§47
Historical Introduction

For a long time in the history of mathematics, algebra was understood to be the study of roots of polynomials.

This must be clearly distinguished from numerical computation of the roots of a given specific polynomial. The Newton-Hörner method is the best known procedure to evaluate roots of polynomials. The actual calculation of roots was (and is) a minor point. The principal object of algebra was understanding the structure of the roots: how they depend on the coefficients, whether they can be given in a formula, etc.

There is, of course, the related question concerning the existence of roots of polynomials. Does every polynomial have a root? Here the coefficient of polynomials were implicitly understood to be real numbers. A. Girard (1595-1632) expressed that any polynomial has a root in some realm of numbers (not neccessarily in the realm of complex numbers), without indicating any method of proof. R. Descartes (1596-1650) noted that $x - c$ is a divisor of a polynomial if c is a root of that polynomial and gave a rule for determining the number of real roots in a specified interval. He makes an obscure remark about the existence of roots. Euler stated that any polynomial has a root in complex numbers. This result came to be called the fundamental theorem of algebra, a very inappropriate name. Euler proved it rigorously for polynomials of degree $\leqslant 6$. J. R. D'Alembert (1717-1783), Lagrange, P. S. Laplace (1749-1827) made attempts to prove this statement. As Gauss criticized, their proof actually assumes the existence of a root in some realm of numbers, and shows that the root is in fact in $\mathbb{C}$. Gauss himself gave several proofs, some of which cannot be accepted as rigorous by modern standards. Nevertheless, Gauss has the credit for having given the first valid demonstration of the so-called fundamental theorem of algebra. After Kronecker established in 1882 that any polynomial has a root is some realm of "numbers" (see §51), the earlier attempts became rigorous proofs. The really fundamental the-orem is Kronecker's theorem.

This assures the existence of roots, but does not bring insight to the problem of understanding the nature of roots any more than existence theorems about differential equations give solutions of differential equations or information about their analytic bahavior, singularities, asymptotic expansions, etc.

The solution of quadratic equations were known to many ancient civilizations. The cubic and biquadratic polynomials (that is, polynomials of degree four) were treated by Italian mathematicians. Scipione del Ferro (1465-1526) succeeded in solving the cubic equation $x^3 + ax = b$ (1515) in terms of radical expresions. In 1535, Tartaglia (1499/1500-1557) solved the cubic polynomial of the form $x^3 + ax^2 = b$. G. Cardan (1501-1576), substituted $x - (b/3)$ for x and transformed the general cubic $x^3 + bx^2 + cx + d$ to a form in which the x^2 term is absent. Thus assuming, with no loss of generality, the equation to be $x^3 + px + q = 0$, a formula for the roots is found to be

$$\sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$$

This is known as Cardan's formula, but it is actually Tartaglia who found it and divulged it to Cardan under pledge of secrecy, who later broke his promise and published it in his book *Ars Magna* (1545). Cardan's originality lay in reducing the general cubic to one of the form $x^3 + px + q$, discussing the so called irreducible case, noting that a cubic can have at most three roots and making an introduction to the theory of symmetric polynomials.

Cardan's book contains a method for finding roots of biquadratic polynomials (that is, polynomials of degree four) discovered by his pupil L. Ferrari (1522-1565) round 1540. This book made a great impact on the developement of algebra. Cardan even calculated with complex numbers, which manifested themselves to be indispensable. Contrary to what one may be at first inclined to believe, there was no need for complex numbers as far as quadratic equations are concerned: mathematicians had declared such equations as $x^2 = -1$ simply unsolvable. However, in Cardan's formula, one has to take square roots of negative numbers even if all the roots are real (the irreducible case). In fact, the roots of a cubic polynomial whose three roots are real cannot be expressed by a formula involving real radicals only (Lemma 59.30).

Thus the first half of 16th century witnessed remarkable achievements in algebra. As late as 1494, Fra Luca Pacioli() had expressed that a cubic equation cannot be solved by radicals, and by 1540 both the cubic and the biquadratic equation was solved by radicals. The next step would be to find a formula for the roots of a quintic polynomial (that is, polynomials of degree five) and, better still, of a polynomial of n-th degree in general.

Other solutions of polynomial equations of the degree $\leqslant 4$ are later given by Descartes, Walter von Tschirnhausen (ca. 1690) and Euler. Noted mathematicians tried in vein to find a formula for the roots of a quintic polynomial. Mathematicians began to suspect that a quintic polynomial equation cannot be solved by radicals.

Lagrange published in 1770-1771 a long paper "Réflexions sur la résolution algébrique des équations" in which he studied extensively all known methods of solutions of polynomial equations. His aim was to derive a general procedure from the known methods for finding roots of polynomials. He treated quadratic, cubic and biquadratic polynomials in detail, and succeeded in subsuming the various methods under one general principle. The roots of a polynomial are expressed in terms of a quantity t, called the *resolvent*, and the resolvent t itself is the root of an auxiliary polynomial, called the *resolvent polynomial*. When the degree of the given polynomial is n, the resolvent polynomial is of degree $(n-1)!$ in x^n. For $n \leqslant 4$, the auxiliary equation has therefore a smaller degree than the polynomial given, and can be solved algebraically (by induction), but for $n \geqslant 5$, solving the auxiliary equation is not easier than to solving the original equation.

The resolvent is a function of the roots which is invariant under some but not all of the permutation of the roots. For example, when the degree is four, $r_1r_2 + r_3r_4$ does not change if the roots r_1,r_2 and r_3,r_4 are interchanged. Lagrange is thus led to the permutation of the roots, i.e., he investigated, without appropriate terminology and notation, the symmetric group on n letters. (Incidentally, the degree of the resolvent polynomial is a divisor of $n!$, the order of the symmetric group. This is how Lagrange came to Theorem 10.9.)

Lagrange noted that, in the successful cases $n \leqslant 4$, the resolvent has the form $r_1 + \alpha r_2 + \cdots + \alpha^{n-1}r_n$, where r_i are the roots of the polynomial and α is a root of $x^n - 1$. This type of a resolvent does not work in case $n = 5$, but it is concievable that expressions of some other kind could work as resolvents. Lagrange studied which type of expressions could be resolvents.

In 1799, P. Ruffini (1765-1822) claimed a proof of the impossibility of solving the general quintic equation algebraically, but whether his proof was rigorous remained controversial. In 1826, Abel gave the first complete proof of this impossibility theorem. His proof consists of two parts. In the first part, he found the general form of resolvents must be as in Lagrange's description for the cubic and biquadratic cases; in the second part, he demonstrated that it can never be a root of a polynomial of fifth degree. He added, without proof, that the general equation cannot be solved algebraically if the degree is greater than 5. In addition to the general equation, Abel also investigated which special equations can be solved by radicals. He proved a theorem which reads, in modern terminology, that an equation is solvable by radicals if the associated Galois group is commutative. It is in this connection that commutative groups are called abelian.

Abel thus finally demonstrated that the *general* equation cannot be solved by radicals. "General polynomial" means that the coefficients are independent variables or, more in the spirit of algebra, indeterminates. Abel's theorem does not say anything about polynomials whose coefficients are fixed complex numbers. But some polynomial equations with constant coefficients of degree five or greater *are* solvable by radicals. What is the criterion for a polynomial equation to be solvable by radicals? This question is resolved by the French mathematician Évariste Galois (1811-1832). With Galois, the principle subject matter of algebra definitely ceased to be polynomial equations. Galois marks the beginning of modern algebra, which means the study of algebraic structures (groups, rings, vector spaces, fields, and many others).

*

*   *

Galois had a short and dramatic life. He began publishing articles when he was a pupil in Lycée (1828). He was a remarkable talent and a difficult student. He wanted to enter the École Polytechnique, but failed twice in the entrance examinations. The reason, he says later, was that the questions were so simple that he refused to answer them. He later entered the École Normale (1829), but expelled from it due to a letter in the student newspaper. His unbearable pride was notorious. He became politicized, was sent to jail for some months, then began a liason with "une coquette de bas étage" and died in an obscure duel (1830).

Galois' achievements have not been appreciated by his contemporaries. He submitted several papers to the French Academy, but these were rejected as unintelligible. It was not until J. Liouville (1809-1882) published his memoirs in 1846 that the world came to know Galois and realize him to be the one of the greatest mathematicians of all time.

Galois associated, with each resolvent equation, a field intermediate between the field of the coefficients of the polynomial and the field of the roots. His ingenious idea is to associate, with the given polynomial and intermediate fields, a series of groups and to translate assertions about fields into group-theoretical statements. This involved the clarification of the field and group concepts. The theory of groups is founded by Galois. He proved that a polynomial equation is solvable by radicals if and only if, in the series of groups, each group is normal and of prime index in the next one, i.e., if and only if the group of the polynomial is solvable in the sense of Definition 27.19 (Theorem 27.25).

It should be noted that this criterion is not an effective procedure to determine actually whether a polynomial equation is solvable by radicals. His contemporaries expected that "the condition of solvability, if it exists, ought to have an external character which can be verified by inspecting the coefficients of a given equation or, all the better, by solving other equations of degrees lower than that of the equation to be solved."[1] His is not a workable test that effectively decides if an equation is solvable by radicals. Galois himself writes: "If now you give me an equation that you have chosen at pleasure, and if you want to know if it is or if it is not solvable by radicals, I need do nothing more than indicate to you the means of answering your question, without wanting to give myself or anyone else the task of doing it. In a word, the calculations are impractical."[2] But this is the whole point. Who cares about solvability of polynomial equations. What Galois achieved, and what his contemporaries failed to appreciate, is a fascinating parallel between the group and field structures. The group-theoretical solvability condition is at best a trivial application of the theory.

This was too big a change in algebra and in mathematics and heralded the end of an era when mathematics was the science of numbers and figures. Ever since the time of Gauss and Galois, mathematics is the science of structures. Galois theory is the first mathematical theory that compares two different structures: fields and groups. It was not easy to follow this developement. Even mathematicians of later generations concieved Galois theory as a tool for answering certain questions in the theory of equations. The first writer on Galois theory who clearly differentiated between the theory and its applications is Heinrich Weber (1842-1913). In his famous text-book on algebra (1894), the exposition of the theory occupies one chapter, its applications another.

The first writer on Galois theory is E. Betti (1823-1892). He published a paper "Sulla risoluzione delle equazioni algebriche" in 1852, in which he closely follows Galois' line. This is more of a commentary than an original exposition. Here the concept of conjugacy and of factor groups made a appeared dimly. Another commentator on Galois theory is J. A. Serret (1819-1885).

Camile Jordan (1838-1922) gave the first exposition of Galois theory that does not follow Galois' own line. With Jordan, emphasis shifted from polynomials to groups. He made many important original contributions. Among other things, he clarified the relationship between irreducible polynomials and transitive groups, developed the theory of transitive groups, defined factor groups as the group of the auxiliary equation, introduced composition series, proved that the composition factors in any two composition series of a solvable group are isomorphic. The group concept became central, but solving polynomial equations still remained as the major concern.

At the same time, Two German mathematicians, L. Kronecker and R. Dedekind (1831-1916), were making very significant contributions to field theory.

Dedekind lectured on Galois theory as early as 1856. He seems to be the first mathematician who realized that the Galois group should be regarded as an automorphism group of a field rather than a group of permutations. In fact, he uses the term "permutation" for what we now call a field automorphism. This means, of course, he very rightly recognized the theory as a theory on fields, not as a theory on polynomials. He introduced the notion of dependence/independence of elements in an extension field over the base field.

Kronecker discussed adjunction in detail. He noted that it is possible to adjoin transcendental elements as well as algebraic ones to a field and proved the important theorem that any polynomial splits into linear factors in some extension field.

Weber carried Kronecker's and Dedekind's ideas further. His exposition, the first modern treatment of the subject, is not restricted to $\mathbb{Q}$, but rather deals with an arbitrary field. He clearly states that the theory is about field extensions and automorphism groups of these extensions. Weber was far ahead of his time. Many mathematicians of his time found his treatment abstract and difficult.

Then came Emil Artin (1898-1962). He combined techniques of linear algebra and field theory. Extensions are sometimes regarded as fields, sometimes as vector spaces, whichever may be convenient. He studied automorphisms of fields, proved that the degree of an extension is equal to the order of the automorphism group, introduced the notion of a Galois extension, and abolished the role of the resolvent (primitive element). This latter was an ugly aspect of the theory about field extensions, remnant of earlier times when the theory has been regarded as one about polynomials. Artin then set up the correspondence between intermediate fields and subgroups of the automorphism group. All computations are eliminated from the theory. Where an earlier writer would spend many pages for the step-by-step adjunction of resolvents to construct a splitting field, we see Artin merely write: "Let E be a splitting field of $f(x)$." With Artin, Galois theory lost all its connections with its past. It is interesting to note that Artin does to applications of the theory to polynomial equations. In his book *Galois Theory*, applications are harshly separated from the main text: they can be no more than an appendix; but Artin does not even condescend to write the appendix himself: this task is relegated to one of his students.

[1] Poisson, quoted from Kiernan's article (see References), page 76.

[2] Galois, quoted from Edwards' book *Galois Theory*, page 81.