5

Fields

The study of the roots of polynomials is intimately related to the study of fields. If $f(x) \in k[x]$, where k is a field, then it is natural to consider the relation between k and the larger field E, where E is obtained from k by adjoining all the roots of $f(x)$. For example, if $E = k$, then $f(x)$ is a product of linear factors in $k[x]$. We shall see that the pair E and k has a *Galois group*, $\mathrm{Gal}(E/k)$, and that this group determines whether there exists a formula for the roots of $f(x)$ which generalizes the quadratic formula.

5.1 CLASSICAL FORMULAS

Revolutionary events were changing the western world in the early 1500s: the printing press had just been invented; trade with Asia and Africa was flourishing; Columbus had just discovered the New World; and Martin Luther was challenging papal authority. The Reformation and the Renaissance were beginning.

The Italian peninsula was not one country but a collection of city states with many wealthy and cosmopolitan traders. Public mathematics contests, sponsored by the dukes of the cities, were an old tradition; there are records from 1225 of Leonardo of Pisa (c. 1180–c. 1245), also called Fibonacci, approximating roots of $x^3 + 2x^2 + 10x - 20$ with good accuracy. One of the problems frequently set involved finding roots of a given cubic equation

$$X^3 + bX^2 + cX + d = 0,$$

where a, b, and c were real numbers, usually integers.[1]

[1] Around 1074, Omar Khayyam (1048–1123), a Persian mathematician now more famous for his poetry, used intersections of conic sections to give geometric constructions of roots of cubics.

5

Fields

The study of the roots of polynomials is intimately related to the study of fields. If $f(x) \in k[x]$, where k is a field, then it is natural to consider the relation between k and the larger field E, where E is obtained from k by adjoining all the roots of $f(x)$. For example, if $E = k$, then $f(x)$ is a product of linear factors in $k[x]$. We shall see that the pair E and k has a *Galois group*, $\mathrm{Gal}(E/k)$, and that this group determines whether there exists a formula for the roots of $f(x)$ which generalizes the quadratic formula.

5.1 CLASSICAL FORMULAS

Revolutionary events were changing the western world in the early 1500s: the printing press had just been invented; trade with Asia and Africa was flourishing; Columbus had just discovered the New World; and Martin Luther was challenging papal authority. The Reformation and the Renaissance were beginning.

The Italian peninsula was not one country but a collection of city states with many wealthy and cosmopolitan traders. Public mathematics contests, sponsored by the dukes of the cities, were an old tradition; there are records from 1225 of Leonardo of Pisa (c. 1180–c. 1245), also called Fibonacci, approximating roots of $x^3 + 2x^2 + 10x - 20$ with good accuracy. One of the problems frequently set involved finding roots of a given cubic equation

$$X^3 + bX^2 + cX + d = 0,$$

where a, b, and c were real numbers, usually integers.[1]

[1] Around 1074, Omar Khayyam (1048–1123), a Persian mathematician now more famous for his poetry, used intersections of conic sections to give geometric constructions of roots of cubics.

Modern notation did not exist in the early 1500s, and so the feat of finding the roots of a cubic involved not only mathematical ingenuity but also an ability to surmount linguistic obstacles. Designating variables by letters was invented in 1591 by F. Viète (1540–1603) who used consonants to denote constants and vowels to denote variables (the modern notation of using letters $a, b, c, \ldots$ at the beginning of the alphabet to denote constants and letters x, y, z at the end of the alphabet to denote variables was introduced in 1637 by R. Descartes in his book *La Géométrie*). The exponential notation $A^2, A^3, A^4, \ldots$ was essentially introduced by J. Hume in 1636 (he used $A^{\text{ii}}, A^{\text{iii}}, A^{\text{iv}}, \ldots$). The symbols $+, -$, and $\sqrt{\ }$, as well as the symbol / for division, as in a/b, were introduced by J. Widman in 1486. The symbol $\times$ for multiplication was introduced by W. Oughtred in 1631, and the symbol $\div$ for division by J. H. Rahn in 1659. The symbol $=$ was introduced by the Oxford don Robert Recorde in 1557, in his *Whetstone of Wit*:

> And to avoide the tediouse repetition of these woordes: is equal to: I will lette as I doe often in woorke use, a paire of paralleles, or gemowe lines of one lengthe, thus: $=$, because noe 2 thynges, can be moare equalle.

(*Gemowe* is an obsolete word meaning *twin* or, in this case, *parallel*.) These symbols were not adopted at once, and often there were competing notations. Most of this notation did not become universal in Europe until the next century, with the publication of Descartes's *La Géométrie*.

Let us return to cubic equations. The lack of good notation was a great handicap. For example, the cubic equation $X^3 + 2X^2 + 4X - 1 = 0$ would be given, roughly, as follows:

> Take the cube of a thing, add to it twice the square of the thing, to this add 4 times the thing, and this must all be set equal to 1.

Complicating matters even more, negative numbers were not accepted; an equation of the form $X^3 - 2X^2 - 4X + 1 = 0$ would only be given in the form $X^3 + 1 = 2X^2 + 4X$. Thus, there were many forms of cubic equations, depending (in our notation) on whether coefficients were positive, negative, or zero.

About 1515, Scipione del Ferro of Bologna discovered a method for finding the roots of several forms of a cubic. Given the competitive context, it was natural for him to keep his method secret. Before his death in 1526, Scipione shared his result with some of his students.

The following history is from the excellent account in J.-P. Tignol, *Galois' Theory of Equations*.