# Cubic

## Historical note

Archeological records show that the ancient Babylonian civilization already knew how to solve quadratic equations. The cubic and quartic equations were subsequently solved *algebraically* in the sixteenth century; that is, their solutions were expressed by formulae involving only addition, subtraction, multiplication, division and the extraction of square roots and cube roots. So it was a great challenge to mathematicians to solve equations of higher degree algebraically until it was first shown in the nineteenth century by Abel, then by Galois, that it is not possible to solve a general quintic equation algebraically. The work of Galois is significant in that he associated a *group* to a given equation and found a criterion for solvability in terms of the *solvability* of the group, whereby the unsolvability of the general quintic was deduced as a special case. The present article demonstrates this idea: the solving of a cubic equation is broken down to solving a quadratic polynomial, extracting cubic roots and solving a system of linear equations, which amounts to the fact the group of a general cubic is solvable. Galois did not live to see the recognition of his celebrated work. His work was published more than ten years after his tragic death.

## The basic idea

Let $f(x) = x^3 - ax^2 + bx - c$

be a cubic polynomial and let and be the roots of $f(x) = 0$. It is well known that the relationship among the roots and coefficients can be described by

$$\begin{cases} e_1 + e_2 + e_3 = a \\ e_1e_2 + e_2e_3 + e_3e_1 = b \\ e_1e_2e_3 = c \end{cases} \qquad \text{(A)}$$

In general, one does not expect to find the roots of $f(x) = 0$ by solving the above system of equations. It is, however, worthwhile to point out that the system (A) reveals the fact that without knowing the actual values of $e_1$, $e_2$ and $e_3$, one can still determine uniquely the values of $e_1 + e_2 + e_3$, $e_1e_2 + e_2e_3 + e_3e_1$ and $e_1e_2e_3$. Hence, it is very natural to ask whether it is possible for us to determine, for appropriate $A_1$, $A_2$, $A_4$ and $A_5$, the values of

$$e_1 + A_1e_2 + A_2e_3$$

and

$$e_1 + A_4e_2 + A_5e_3.$$

Set

$$A_3 = e_1 + A_1e_2 + A_2e_3$$

and

$$A_6 = e_1 + A_4e_2 + A_5e_3.$$

*by*

***Cheng Kai Nah***

***Lang Mong Lung***

*Both authors are Senior Lecturers at the Department of Mathematics, National University of Singapore.*

Successful determination of $A_1$, $A_2$, $A_4$, $A_5$, $A_3$ and $A_6$ will consequently provide us the following system of linear equations:

$$\begin{cases} e_1 + e_2 + e_3 = a \\ e_1 + A_1e_2 + A_2e_3 = A_3 \\ e_1 + A_4e_2 + A_5e_3 = A_6 \end{cases} \qquad \text{(B)}$$

This will of course enable us to write down the explicit formulae for $e_1$, $e_2$ and $e_3$ if

$$\det \begin{bmatrix} 1 & 1 & 1 \\ 1 & A_1 & A_2 \\ 1 & A_4 & A_5 \end{bmatrix} \neq 0.$$

## Permutations and Symmetric Polynomials

Denote by $I$ the set {1, 2, 3}. A permutation $\sigma$ of the set $I$ is a bijective function from $I$ onto $I$ itself. It is easy to see that there are altogether 6 permutations:

$$\sigma_1(1) = 1,\ \sigma_1(2) = 2,\ \sigma_1(3) = 3,$$

$$\sigma_2(1) = 1,\ \sigma_2(2) = 3,\ \sigma_2(3) = 2,$$

$$\sigma_3(1) = 2,\ \sigma_3(2) = 1,\ \sigma_3(3) = 3,$$

$$\sigma_4(1) = 2,\ \sigma_4(2) = 3,\ \sigma_4(3) = 1,$$

$$\sigma_5(1) = 3,\ \sigma_5(2) = 1,\ \sigma_5(3) = 2,$$

$$\sigma_6(1) = 3,\ \sigma_6(2) = 2,\ \sigma_6(3) = 1.$$

(That is, $\sigma_1$ fixes each of the digits 1, 2 and 3, $\sigma_2$ sends 1 to 1, 2 to 3 and 3 to 2, etc.)

Let $x_1$, $x_2$ and $x_3$ be three indeterminates. A monomial in $x_1$, $x_2$ and $x_3$ is an expression of the form

$$ax_1^bx_2^cx_3^d$$

where $a$ is a nonzero complex number and $b$, $c$, $d$ are nonnegative integers. A sum of finitely many monomials (in $x_1$, $x_2$ and $x_3$) is called a polynomial (in $x_1$, $x_2$ and $x_3$).

Let $\sigma$ be a permutation on $I$. Then $\sigma$ permutes the monomials in a natural way. Namely, for $m = ax_1^bx_2^cx_3^d$,

$$\sigma(m) = ax_{\sigma(1)}^b x_{\sigma(2)}^c x_{\sigma(3)}^d.$$

And in turn for each polynomial $p = m_1 + m_2 + \ldots + m_k$ where the $m_i$'s are monomials, we define

$$\sigma(p) = \sigma(m_1) + \sigma(m_2) + \ldots + \sigma(m_k).$$

**Example 1**

$$\sigma_4(x_1x_2) = x_{\sigma_4(1)}x_{\sigma_4(2)} = x_2x_3.$$

**Example 2**

$$\sigma_4(x_1x_2 - 10x_1^3x_2x_3) = x_2x_3 - 10x_2^3x_3x_1.$$

**Definition**

A *symmetric polynomial* is a polynomial $p = p(x_1, x_2, x_3)$ such that $\sigma_i(p) = p$ for each $i$ with $1 \leq i \leq 6$.

One sees easily that $x_1 + x_2 + x_3$, $x_1x_2 + x_2x_3 + x_3x_1$ and $x_1x_2x_3$ are symmetric polynomials while $x_1x_2$ is not since

$$\sigma_4(x_1x_2) = x_2x_3 \neq x_1x_2.$$

And the following result is clearly true.

**Lemma 1**

Let $p_1$ and $p_2$ be symmetric polynomials. Then $p_1 + p_2$, $p_1 - p_2$ and $p_1p_2$ are symmetric polynomials.

Denote by $M_1$, $M_2$ and $M_3$ the symmetric polynomials $x_1 + x_2 + x_3$, $x_1x_2 + x_2x_3 + x_3x_1$ and $x_1x_2x_3$ respectively. They are known as the *elementary symmetric* polynomials due to the following result of Newton.

**Theorem 2**

Every symmetric polynomial $p(x_1, x_2, x_3)$ can be expressed in terms of $M_1$, $M_2$ and $M_3$.

**Example 3**

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 + (x_1x_2 + x_2x_3 + x_3x_1)^2 \\ &= M_1^2 - 2M_2. \end{aligned}$$

## Symmetric Polynomials Involving $x_1 + Bx_2 + Cx_3$

One sees easily that the polynomial $x_1 + Bx_2 + Cx_3$ is symmetric if and only if $1 = B = C$. But what if $B$ and $C$ are distinct from 1, can one construct a symmetric polynomial which involves $p = x_1 + Bx_2 + Cx_3$? This is a crucial step in Galois' construction.

There are many different ways to construct such symmetric polynomials. Here is one of such constructions that turns out to be very useful to us.

Let's consider how $p$ is permuted by all the permutations on $I$:

$$\sigma_1(p) = x_1 + Bx_2 + Cx_3,$$

$$\sigma_2(p) = x_1 + Bx_3 + Cx_2,$$

$$\sigma_3(p) = x_2 + Bx_1 + Cx_3,$$

$$\sigma_4(p) = x_2 + Bx_3 + Cx_1,$$

$$\sigma_5(p) = x_3 + Bx_1 + Cx_2,$$

and

$$\sigma_6(p) = x_3 + Bx_2 + Cx_1.$$

One can check easily that

$$U(B, C) + V(B, C)$$

and

$$U(B, C)\, V(B, C)$$

are symmetric polynomials where

$$U(B, C) = (x_2 + Bx_3 + Cx_1)(x_3 + Bx_1 + Cx_2)(x_1 + Bx_2 + Cx_3)$$

and

$$V(B, C) = (x_2 + Bx_1 + Cx_3)(x_3 + Bx_2 + Cx_1)(x_1 + Bx_3 + Cx_2)$$

By Theorem 2, we may write both $U(B, C) + V(B, C)$ and $U(B, C)\, V(B, C)$ into polynomials in terms of $M_1$, $M_2$ and $M_3$.

Replacing $x_1$, $x_2$ and $x_3$ by $e_1$, $e_2$ and $e_3$ respectively and using (A), we may further express both $U(B, C) + V(B, C)$ and $U(B, C)\, V(B, C)$ in terms of $B$, $C$, $a$, $b$ and $c$. Set

$$U(B, C) + V(B, C) = g$$

and

$$U(B, C)\, V(B, C) = h.$$

Then $U(B, C)$ and $V(B, C)$ are roots of the quadratic polynomial

$$x^2 - gx + h.$$

Applying the quadratic roots formula, we can solve for $U(B, C)$ and $V(B, C)$.

The next crucial step lies in the realization that by choosing

$$B = \omega = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}, \text{ where } i^2 = -1,$$

and

$$C = \omega^2,$$

$U(B, C)$ and $V(B, C)$ become cubic powers:

$$U(B, C) = (e_1 + Be_2 + Ce_3)^3$$
$$V(B, C) = (e_1 + Ce_2 + Be_3)^3.$$

Consequently, $(e_1 + Be_2 + Ce_3)$ and $(e_1 + Ce_2 + Be_3)$ can be determined.

### The roots of $f(x) = x^3 - ax^2 + bx - c$

Direct calculation shows that

$$g = U + V = U(\omega, \omega^2) + V(\omega, \omega^2) = 2a^3 - 9ab + 27c$$

and

$$h = UV = U(\omega, \omega^2)V(\omega, \omega^2) = (a^2 - 3b)^3.$$

So that

$$U = (e_1 + \omega e_2 + \omega^2 e_3)^3$$

and

$$V = (e_1 + \omega^2 e_2 + \omega e_3)^3$$

are the roots of the quadratic polynomial

$$x^2 - (2a^3 - 9ab + 27c)x + (a^2 - 3b)^3.$$

Note that this quadratic polynomial is determined uniquely by the given cubic polynomial $f(x) = x^3 - ax^2 + bx - c$. We may now apply the quadratic root formula to determine the values $(e_1 + \omega e_2 + \omega^2 e_3)$ and $(e_1 + \omega^2 e_2 + \omega e_3)$. As a consequence, we obtain the following system of linear equations:

$$\begin{cases} e_1 + e_2 + e_3 = a \\ e_1 + \omega e_2 + \omega^2 e_3 = ((g + (g^2 - 4h)^{1/2})/2)^{1/3} \\ e_1 + \omega^2 e_2 + \omega e_3 = ((g - (g^2 - 4h)^{1/2})/2)^{1/3} \end{cases}$$

where

$$g = 2a^3 - 9ab + 27c$$

and

$$h = (a^2 - 3b)^3.$$

Moreover

$$\det \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \neq 0.$$

It is now clear that the cubic equation

$$f(x) = 0$$

is solved.

**Remark** One may start directly from the system of linear equations

$$\begin{cases} e_1 + e_2 + e_3 = a \\ e_1 + \omega e_2 + \omega^2 e_3 = A_3 \\ e_1 + \omega^2 e_2 + \omega e_3 = A_6 \end{cases}$$

to shorten the lengthy discussion we presented in this article. Then all one has to do is to determine the values $A_3$ and $A_6$. M²

### Further Reading

Stewart, Ian, *Galois Theory*, Chapman and Hall 1973.

Stillwell, John, *Elements of Algebra*, Springer-Verlag 1994.