Casus irreducibilis and *Maple*

Rudolf Výborný

Abstract

We give a proof that there is no formula which uses only addition, multiplication and extraction of real roots on the coefficients of an irreducible cubic equation with three real roots that would provide a solution.

1 Introduction

The Cardano formulae for the roots of a cubic equation with real coefficients and three real roots give the solution in a rather complicated form involving complex numbers. Any effort to simplify it is doomed to failure; trying to get rid of complex numbers leads back to the original equation. For this reason, this case of a cubic is called casus irreducibilis: the irreducible case. The usual proof uses the Galois theory [3]. Here we give a fairly simple proof which perhaps is not quite elementary but should be accessible to undergraduates. It is well known that a convenient solution for a cubic with real roots is in terms of trigonometric functions. In the last section we handle the irreducible case in *Maple* and obtain the trigonometric solution.

2 Prerequisites

By $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ we denote the natural numbers, the rationals, the reals and the complex numbers, respectively. If F is a field then $F[X]$ denotes the ring of polynomials with coefficients in F. If $F \subset \mathbb{C}$ is a field, $a \in \mathbb{C}$ but $a \notin F$ then there exists a smallest field of complex numbers which contains both F and a, we denote it by $F(a)$. Obviously it is the intersection of all fields which contain F as well as a. We say that $F(a)$ was generated by adjunction of the element a to the field F. If $T(x)$ is a polynomial irreducible in $F[X]$, or, as we may also say irreducible over F, and $T(a) = 0$ then $F(a)$ is the set of elements of the form $P(a)$, where $P(x)$ is some polynomial in $F[X]$. This reprezentation is unique, provided that $\deg P < \deg T$. If $T(b) = 0$ also then $F(a)$ and $F(b)$ are isomorphic; the isomorphism I_σ is defined by $I_\sigma(P(a)) = P(b)$. If F_1 and F_2 are two isomorphic fields then $F_1[X]$ and $F_2[X]$ are also isomorphic, in case of $F(a)[X]$ and $F(b)[X]$ this isomorphism is given by

$$a_n x^n + \cdots a_1 x + a_0 \longmapsto I_\sigma(a_n)x^n + \cdots I_\sigma(a_1)x + I_\sigma(a_0).$$

Detailed explanations and proofs can be found in text on abstract algebra, for instance [1] or [2].

We now prove two theorems which are needed for the main result.

Theorem 1 *Let p be a prime, $F \subset \mathbb{C}$ a field. If c is not a p-th power of an element in F then the polynomial $x^p - c$ is irreducible in $F[X]$.*

Proof Assume, contrary to what we want to prove, that

$$x^p - c = h(x)g(x),$$

with $h(x)$ and $g(x)$ in $F[X]$ and $1 < \deg h(x) < p$. Let

$$\varepsilon = \cos\frac{2\pi}{p} + \imath \sin\frac{2\pi}{p} \tag{1}$$

and w be a fixed complex number satisfying $w^p = c$. Then the roots of the equation $x^p = c$ are

$$w,\ w\varepsilon,\ w\varepsilon^2, \dots, w\varepsilon^{p-1}.$$

Consequently

$$(x-w)(x-w\varepsilon)\dots(x-w\varepsilon^{p-1}) = h(x)g(x).$$

The absolute term A of the polynomial $h(x)$ lies in F and is of the form $A = \varepsilon^k w^j$ with $j < p$ and k, j positive integers. Hence $A^p = \varepsilon^{kp} w^{pj} = c^j$. Since p, j are relatively prime there are integers α, β such that $\alpha j + \beta p = 1$. Consequently

$$c = c^{\alpha j + \beta p} = c^{\alpha j} c^{\beta p} = A^{\alpha p} c^{\beta p} = (A^\alpha c^\beta)^p.$$

This contradicts the assumption that c is not a p-th power of an element in F.

Theorem 2 *Let $F \subset \mathbb{C}$ be a field and $f(x)$, $g(x) \in F[X]$. If $f(x)$ is irreducible and $f(a) = g(a) = 0$ for some complex number a then $f(x)$ divides $g(x)$.*

Proof We can and shall assume that $g(x)$ is not a zero polynomial. Then there exists a greatest common divisor $d(x)$ of $f(x)$ and $g(x)$, the coefficients of $d(x)$ are in F. Clearly $d(a) = 0$ and consequently $\deg d(x) \geq 1$. Since $f(x)$ is irreducible it divides $d(x)$ and hence $f(x)$ divides $g(x)$.

3 The Theorem

In this section we wish to prove that there is no formula, which uses only real numbers, addition, multiplication, subtraction, division and extraction of roots and provides the solution to any cubic equations with three real roots. Firstly, we rephrase and make this statement more precise. Let $T(x)$ be a cubic polynomial with rational coefficients, irreducible in $\mathbb{Q}[X]$. If such a formula existed it would be possible to find a finite sequence of fields, F_1, $F_2, \dots F_m$ such that

(1) $F_1 = \mathbb{Q}$;
(2) For $i = 2, \dots, m$ the field F_i is created by adjunction of a *real* root of an equation of the form $x^p = c$, with c in F_{i-1};
(3) $T(x)$ is irreducible over F_i for $i = 1, \dots, m-1$;
(4) $T(x)$ has a root (or simply ceases to be irreducible) in F_m.

Remark The number p, as the notation suggests, can be always taken to be a prime. If we wish to adjunct e. g. $\sqrt[12]{7}$ we adjunct succesively $\sqrt{7}$, $\sqrt{\sqrt{7}}$ and $\sqrt[3]{\sqrt{\sqrt{7}}}$.

Theorem 3 (Casus irreducibilis) *Let $T(x)$ be a cubic polynomial irreducible over $\mathbb{Q}$ and F_1, $F_2, \dots F_m$ be fields satisfying* 1.–4. *Then $T(x)$ has two roots with non-zero imaginary parts.*

Remark If $T(x)$ has three real roots then the chain of fields as in 1.–4. cannot exist. Therefore the roots of $T(x)$ are not expressible in terms of real roots.

Proof of Theorem 3. Let r be the real root of the equation $x^p = c$ with $c \in F_{m-1}$ and ε as in (1). Since $T(x)$ is irreducible over F_{m-1} but reducible over F_m there is a polynomial $P(x) = a_0 + a_1 x + \cdots a_{p-1} x^{p-1}$ with $a_i \in F_{m-1}$ such that

$$T(x) = (x - P(r))Q(x),$$

where $Q(x)$ is a quadratic polynomial with coefficients in F_m. Now let

$$S(x) = (x - P(r))(x - P(r\varepsilon)) \cdots (x - P(r\varepsilon^{p-1})).$$

The coefficient b_k of x^k in $S(x)$ is $\sigma_k(P(r), \dots, P(r\varepsilon^{p-1}))$, where $\sigma_k(x_1, \dots, x_p)$ is the kth elementary symmetric polynomial. Since $\sigma_k(P(y_1), \dots, P(y_p))$ is a symmetric polynomial with coefficients in F_{m-1}, it follows by the fundamental theorem on symmetric polynomials (see e. g [2] p.314) that there exists a polynomial $B_k(u_1, \dots, u_p)$ with coefficients in F_{m-1} such that

$$\sigma_k(P(y_1), \dots, P(y_p)) = B_k(\sigma_1(y_1, \dots, y_p), \dots, \sigma_k(y_1, \dots, y_p)).$$

We note that $\sigma_i(r, \dots, r\varepsilon^{p-1})$ is the ith coefficient of $x^p - c$. Substituting $y_k = r\varepsilon^{k-1}$ in the above equation we have that $b_k \in F_{m-1}$ for $k = 1, \dots, p$. Since $T(x)$ is irreducible over F_{m-1} and $S(x)$ and $T(x)$ have a common root (namely $P(r)$), $T(x)$ must divide $S(x)$. Since $F_{m-1}(r\varepsilon^k)$ is isomorphic to F_m all the numbers $P(r\varepsilon^k)$ are roots of $T(x)$. If degree of $S(x)/T(x)$ is not zero it will again have a common root with $T(x)$ and consequently be divisible by $T(x)$. Continuing with this process we come to the conclusion that there is a positive integer n and $a \neq 0$ such that $S(x) = a[T(x)]^n$ for some natural n. Consequently $p = 3n$ and since p is a prime $p = 3$ and $n = 1$. Therefore we have

$$\begin{aligned} aT(x) &= S(x) \\ &= (x - (b_0 + b_1 r + b_2 r^2))(x - (b_0 + b_1 r\varepsilon + b_2 r^2\varepsilon^2))(x - (b_0 + b_1 r\varepsilon^2 + b_2 r^2\varepsilon)), \qquad (2) \end{aligned}$$

with real numbers b_0, b_1, b_2. Since $\Re\varepsilon = \Re\varepsilon^2$ the real parts of

$$b_0 + b_1 r\varepsilon + b_2 r^2\varepsilon^2 \text{ and } b_0 + b_1 r\varepsilon^2 + b_2 r^2\varepsilon$$

are also equal, hence their imaginary parts cannot be zero, otherwise $T(x)$ would have a double root, contrary to the assumption that it is irreducible. Therefore two roots of $T(x) = 0$ are imaginary.

4 Maple and the cubic

The *Maple* command `solve` provides a satisfactory solution for the cubic except in the case of an irreducible cubic with three real roots. In this case the answer is equivalent to the use of Cayley's form of the Cardano formulae; the roots are given in a complex form unsuitable for use in further computation. We have shown that there is no point in trying to get rid of the complex numbers. This has ramifications beyond cubics: if we are to solve an algebraic equation which has several irreducible cubic factors with three real roots, the solve command will give all roots of these factors in an inconvient form. All problems disappear with the numerical solution, however in some situation one might want to have a solution in a 'closed form.'

The so called trigonometric solution was used for solving the cubic with three real roots before the age of computer algebra system. Although *Maple* does not provide this form of the solution directly it is possible to obtain from *Maple* an 'exact' solution in terms of trigonometric functions. A convenient way of proceeding is to put the result of the `solve` command in a list and then use the command `evalc` on the list (following possibly with the `simplify` command).

References

[1] N.H. McCoy *Fundamentals of Abstract Algebra* (Allyn and Bacon Boston 1972)
[2] A. Kurosh *Higher Algebra* (Mir Moscow 1980)
[3] B.L. Van der Waerden, Moderne Algebra I (Berlin 1930).

Department of Mathematics, University of Queensland, St Lucia, QLD 4072
E-mail: rudolf.vyborny@mailbox.uq.edu.au

Received 23 June 2004, accepted 27 October 2004.