Factoring Cubic Polynomials

Robert G. Underwood

1. Introduction

There are at least two ways in which using the famous *Cardano formulas* (1545) to factor cubic polynomials present more difficulties than the quadratic formula poses when factoring quadratic polynomials. First and obviously, with its cube roots and roots of roots, the Cardano formulas involve computations that are more complicated. Second, we get less in return; in particular, with the Cardano formulas we only obtain one out of three factors, whereas the quadratic formula yields both factors of any given quadratic polynomial. In this paper, we will describe a natural procedure that will lead us to all three factors of an arbitrary cubic polynomial with real number coefficients.

Let $\mathbf{R}$ denote the real field, and let $\mathbf{R}[X]$ denote the ring of polynomials over $\mathbf{R}$. Consider the cubic polynomial $p(X) = X^3 - k \in \mathbf{R}[X]$. Let $\mathbf{C}$ denote the field of complex numbers, and let ζ be a primitive 3rd root of unity, that is, ζ is one of the two complex solutions of the equation $X^3 = 1$. One calculates $\zeta = \dfrac{-1 + i\sqrt{3}}{2}$, where $i = \sqrt{-1}$.

The cubic $p(X)$ factors completely over $\mathbf{C}$. Indeed, if $\sqrt[3]{k}$ is the real 3rd root of k, then we have the factorization

$$X^3 - k = (X - \sqrt[3]{k})(X - \zeta\sqrt[3]{k})(X - \zeta^2\sqrt[3]{k}),$$

and the roots of $X^3 - k$ are $\sqrt[3]{k}$, $\zeta\sqrt[3]{k}$, $\zeta^2\sqrt[3]{k}$.

In this paper we show how to generate the roots of *any* cubic polynomial over $\mathbf{R}$ in an analogous manner, using ζ, and a solution (a, b) of the equation $X^3 + Y^3 = 1$ over $\mathbf{C}$.

2. Generating the roots of a cubic polynomial

The problem of finding all the zeros of an arbitrary monic cubic polynomial

$$f(X) = X^3 + \alpha X^2 + \beta X + \gamma$$

is equivalent to the problem of finding the zeros of the reduced cubic

$$g(X) = X^3 + \delta X + \epsilon.$$

We see that if c is a zero of $g(X)$, then $c - (1/3)\alpha$ will be a zero of $f(X)$, cf. [3, p. 568]. It is not difficult to show that any reduced cubic can be written in the form

$$p(X) = X^3 - 3k^2abX + k^3$$

where $(a, b) \in \mathbf{C} \times \mathbf{C}$ is a solution to the equation $X^3 + Y^3 = 1$. For example, if $p(X) = X^3 - 12X + 8$, we choose $k = 2$ and a and b so that $a^3 + b^3 = 1$ with $ab = 1$. Hence the required solution is $(a, 1/a)$, where a is the root

$$a = \sqrt[3]{\frac{1}{2} + \frac{i\sqrt{3}}{2}}$$

of the quadratic equation in X^3: $X^6 - X^3 + 1 = 0$.

With this in mind, we prove the following:

Theorem. *Suppose $p(X)$ is a reduced cubic in the form*

$$p(X) = X^3 - 3k^2abX + k^3$$

where (a, b) is a solution of the equation $X^3 + Y^3 = 1$, and k is a real number. Then the roots of $p(X)$ are

$$\begin{aligned} c_1 &= -ka - kb \\ c_2 &= -ka\zeta - kb\zeta^2 \\ c_3 &= -ka\zeta^2 - kb\zeta. \end{aligned}$$

Proof. One could show directly that $p(c_i) = 0$ for $i = 1, 2, 3$, but we present a different proof.

Consider $\mathbf{C}^3$, the vector space generated by ordered triples (r, s, t) of complex numbers. Set $r = ka$, $s = kb$, and $t = c_1 = -ka - kb$. Then the set

$$S = \{(ka, kb, t), (t, ka, kb), (kb, t, ka)\}$$

is linearly dependent over $\mathbf{C}$. To see this, observe that:

$$(-1)(ka, kb, c_1) + (-1)(c_1, ka, kb) = (kb, c_1, ka)$$

is a dependence relation. It follows that the matrix

$$A = \begin{bmatrix} ka & kb & c_1 \\ c_1 & ka & kb \\ kb & c_1 & ka \end{bmatrix}$$

is singular, since the rows of A are linearly dependent. Thus

$$\det(A) = k^3a^3 + k^3b^3 + c_1^3 - 3k^2abc_1 = 0,$$

which we may rewrite as

$$k^3a^3 + k^3b^3 - k^3 + (c_1^3 - 3k^2abc_1 + k^3) = 0, \quad \text{or}$$

$$c_1^3 - 3k^2abc_1 + k^3 = 0,$$

since (a, b) is a solution of $X^3 + Y^3 = 1$. We conclude that $c_1 = -ka - kb$ is a root of our reduced cubic $p(X) = X^3 - 3k^2abX + k^3$.

To find the other roots of the cubic $p(X)$, we find other values of t so that the set

$$S = \{(ka, kb, t), (t, ka, kb), (kb, t, ka)\}$$

is linearly dependent. Another such value is $t = c_2 = -ka\zeta - kb\zeta^2$. To see this, observe that the set S is linearly dependent via the relation

$$(-\zeta^2)(ka, kb, c_2) + (-\zeta)(c_2, ka, kb) = (kb, c_2, ka).$$

The matrix

$$A = \begin{bmatrix} ka & kb & c_2 \\ c_2 & ka & kb \\ kb & c_2 & ka \end{bmatrix}$$

is singular, and

$$\det(A) = k^3a^3 + k^3b^3 + c_2^3 - 3k^2abc_2 = 0,$$

which, in turn, implies that

$$c_2^3 - 3k^2abc_2 + k^3 = 0.$$

Thus c_2 is the second root of $p(X)$.

Finally, if we put $t = c_3 = -ka\zeta^2 - kb\zeta$ the set

$$S = \{(ka, kb, t), (t, ka, kb), (kb, t, ka)\}$$

is linearly dependent via the relation

$$(-\zeta)(ka, kb, c_3) + (-\zeta^2)(c_3, ka, kb) = (kb, c_3, ka).$$

The matrix

$$A = \begin{bmatrix} ka & kb & c_3 \\ c_3 & ka & kb \\ kb & c_3 & ka \end{bmatrix}$$

is singular, and

$$\det(A) = k^3a^3 + k^3b^3 + c_3^3 - 3k^2abc_3 = 0,$$

which, in turn, implies that

$$c_3^3 - 3k^2abc_3 + k^3 = 0.$$

Thus c_3 is the third and last root of $p(X)$. $\diamond$

Returning to our example $p(X) = X^3 - 12X + 8$, we obtain the factorization

$$p(X) = (X + 2a + 2a^{-1})(X + 2\zeta a + 2\zeta^2 a^{-1})(X + 2\zeta^2 a + 2\zeta a^{-1}),$$

where

$$a = \sqrt[3]{\frac{1}{2} + \frac{i\sqrt{3}}{2}}.$$

We close with a final thought. Let $\mathbf{Q}$ denote the rational numbers. Suppose $p(X) = X^3 - 3k^2abX + k^3$ is a reduced cubic over $\mathbf{Q}$ with exactly one rational root with $k^2ab \neq 0$. Because Fermat's Last Theorem is true for the case $n = 3$, there are no non-trivial solutions to the equation $X^3 + Y^3 = 1$ in $\mathbf{Q} \times \mathbf{Q}$. Hence if we use our cubic formula to calculate this rational zero, we must involve non-rational reals or non-real complex numbers. We wonder if this is the case using the standard cubic formula, see [3, Theorem 51.3].

References

[1] K. Hoffman, R. Kunze, *Linear Algebra*, Second Edition, Prentice-Hall, New Jersey, 1971.

[2] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory,* Second Edition, Springer-Verlag, New York, 1990.

[3] S. Warner, *Modern Algebra, Vol. II,* Prentice-Hall, New Jersey, 1965.

Department of Mathematics
Auburn University Montgomery
Montgomery, AL 36124
underw@strudel.aum.edu