Queen Mary University of London

MTH4104 **Introduction to Algebra**

Solving polynomial equations **Spring 2021**

In Section 4.3 of the notes, we showed how to solve linear equations in any field K. What about *quadratic equations*? Let's consider the general quadratic equation

$$\alpha z^2 + \beta z + \gamma = 0$$

with coefficients $\alpha, \beta, \gamma \in K$. Can we solve this equation inside K?

The usual solution to the quadratic equation starts by *completing the square*, as follows:

$$\begin{aligned}
\alpha z^2 + \beta z + \gamma &= 0 && \Rightarrow \\
z^2 + \left(\frac{\beta}{\alpha}\right) z + \left(\frac{\gamma}{\alpha}\right) &= 0 && \Rightarrow \\
z^2 + \left(\frac{\beta}{\alpha}\right) z + \frac{\beta^2}{4\alpha^2} + \left(\frac{\gamma}{\alpha}\right) &= \frac{\beta^2}{4\alpha^2} && \Rightarrow \\
\left(z + \frac{\beta}{2\alpha}\right)^2 &= \frac{\beta^2}{4\alpha^2} - \frac{\gamma}{\alpha} = \frac{\beta^2 - 4\alpha\gamma}{4\alpha^2}.
\end{aligned}$$

So far everything we have done is justified by the field axioms. We have divided through by α, which is legal provided that $\alpha \neq 0$ (but if $\alpha = 0$ then we didn't truly have a quadratic). We have added some constants to both sides of the equation, and used associative, inverse, and identity laws several times in a way that the notation mostly masks. So everything so far is correct in K.

Now would come the extraction of the square roots of $\beta^2 - 4\alpha\gamma$, if we were working over the real numbers. (In the denominator we have $\sqrt{4\alpha^2} = \pm 2\alpha$. These are manifestly square roots, and in a field there can be no more square roots, because it can be proved using Proposition 4.7 that the quadratic equation $x^2 - 4\alpha^2 = 0$ can have no more than two solutions.)

Let us suppose for the moment that all square roots exist in K, and we know how to find them. Using $\sqrt{\beta^2 - 4\alpha\gamma}$ to mean any element $u \in K$ satisfying the equation $u^2 = \beta^2 - 4\alpha\gamma$, we can complete the solution as follows:

$$\begin{aligned}
\left(z + \frac{\beta}{2\alpha}\right)^2 &= \frac{\beta^2 - 4\alpha\gamma}{4\alpha^2} && \Rightarrow \\
z + \frac{\beta}{2\alpha} &= \pm\sqrt{\frac{\beta^2 - 4\alpha\gamma}{4\alpha^2}} && \Rightarrow \\
z &= \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}.
\end{aligned}$$

The rest of these derivations work in K as well. So we see that we have reduced solving quadratic equations over K to the problem of extracting square roots inside K.

So, can we extract these square roots? This does *not* follow from the field axioms, and in fact the square roots may or may not exist. After all, $\mathbb{R}$ is a field, but negative numbers have no square roots in $\mathbb{R}$. In $\mathbb{C}$ it follows from the Fundamental Theorem of Algebra that the square roots exist, but that still doesn't help us find them. It turns out that there is a way to compute square roots of complex numbers, and indeed roots of any order, using De Moivre's theorem. This was taught in *Numbers, Sets and Functions*, so I will go no further with it.

And what about polynomial equations of degree greater than two? For *cubic equations*, 16th century Italian algebraists Niccòlo Tartaglia, Scipione del Ferro and others discovered procedures for obtaining solutions similar to what we have just done for the quadratic, involving extraction of square roots and cube roots. Their procedure is sketched below as an exercise, for you to fill in the details. For *quartic equations* there is a procedure as well, usually credited to Lodovico Ferrari around the same time, using square, cube, and fourth roots. But the quartic is the end of the line!

Theorem 0.1 (Abel–Ruffini Theorem) *Let $n \geq 5$ be an integer. There is no expression built from the complex coefficients $a_0, a_1, \ldots, a_n$ using complex scalars, addition, subtraction, multiplication, division, and extraction of roots which evaluates, for all $a_0, a_1, \ldots, a_n \in \mathbb{C}$, to a complex root of the polynomial*

$$a_n x^n + \cdots + a_1 x + a_0.$$

Of course, the Fundamental Theorem of Algebra guarantees that complex solutions exist to the polynomial in the Abel–Ruffini theorem. It is in writing these solutions down that the problem lies.

A proof of the Abel–Ruffini Theorem will be found in a module or textbook on *Galois theory*. At Queen Mary, the module title is "Further Topics in Algebra".

Exercise: the cubic formula This is an involved exercise provided for the benefit of those interested, on how you would derive the cubic formula. Its technique is the one developed by François Viète (French, 1540–1603), the first mathematician to introduce a systematic notation for algebra. It works in any field in which you can take square and cube roots: the only field like this we've discussed so far is $\mathbb{C}$, so I've written the exercise for $\mathbb{C}$.

Let $\alpha, \beta, \gamma, \delta$ be complex numbers, and consider the general cubic equation

$$\alpha x^3 + \beta x^2 + \gamma x + \delta = 0.$$

Suppose that $\alpha \neq 0$.

(a) Consider the substitution $x = y - \beta/3\alpha$ where y is a new variable. Then y also satisfies a cubic equation of the form

$$y^3 + py + q = 0$$

for some complex numbers p, q. Express p and q in terms of α, β, γ and δ.

(b) Consider the substitution $y = z - p/3z$. Prove that z satisfies the equation

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

(c) Using the quadratic formula, find an expression for z^3 (and therefore for z) in terms of p and q.

(d) Using the method explained in this question, solve the cubic equation

$$x^3 + 6x + 2 = 0.$$

Have you found all solutions?