Invariant Theory and Quadratic Polynomials

In this page, aimed at the general reader, we will present a connection between invariant theory and the solution of quadratic equations. At the beginning, our development will seem unmotivated, but we ask the reader to temporarily engage in a willing suspension of disbelief.

Suppose we begin with a quadratic equation

$$p(x) = ax^2 + bx + c = 0$$

where a, b, and c are rational numbers, i.e., fractions (or integers).

Let this equation have (unknown) solutions r and s. Then, whatever r and s are, we may factor the polynomial $p(x) = ax^2 + bx + c$ as

$$ax^2 + bx + c = a(x - r)(x - s) = ax^2 - a(r + s)x + ars.$$

Comparing coefficients on the left-hand and right-hand sides of this equation, we see that

$$r + s = -b/a \qquad \text{and} \qquad rs = c/a.$$

Let us compute the *discriminant* Δ of the polynomial $p(x)$, which by definition is $\Delta = (r - s)^2$. We see that

$$\begin{aligned}\Delta = (r - s)^2 = r^2 - 2rs + s^2 = r^2 + 2rs + s^2 - 4rs &= (r + s)^2 - 4rs \\ &= (-b/a)^2 - 4c/a = (b^2 - 4ac)/a^2.\end{aligned}$$

We then have the following theorem of Galois theory:

Theorem. *The polynomial $p(x) = ax^2 + bx + c$, with a, b, and c rational numbers, has roots r and s that are rational numbers exactly when its discriminant Δ is a rational number that is a perfect square.*

The point of this theorem is the following: We have found a criterion for $p(x)$ to have rational roots *without* having to first find these roots, and furthermore our criterion involves an invariant Δ which we can compute purely in terms of the coefficients of $p(x)$.

Let us observe that the denominator a^2 of Δ is visibly a perfect square, so that Δ is a perfect square exactly when its numerator $b^2 - 4ac$ is a perfect square.

Of course, we know how to solve quadratic equations. We recall the quadratic formula: The equation $ax^2 + bx + c = 0$ has solutions

$$r = (-b + \sqrt{b^2 - 4ac})/2a \qquad \text{and} \qquad s = (-b - \sqrt{b^2 - 4ac})/2a.$$

We can see from these formulas that r and s are rational numbers exactly when $b^2 - 4ac$ is a perfect square, and we can compute $r - s = \sqrt{b^2 - 4ac}/a$, so $\Delta = (r - s)^2 = (b^2 - 4ac)/a^2$, verifying our statements above.

Thus in the simple case of a quadratic polynomial we could have proceeded directly and did not need the general theory developed above. But in the more complicated cases of a cubic or quartic polynomial it is much more expeditious to use the general theory, and in the case of a quintic polynomial, or of a polynomial of higher degree, it is absolutely necessary to use the general theory, as in those cases there is no method for finding the roots of a polynomial.

The discriminant Δ is an example of an *invariant*. In general, by an invariant we mean some quantity that is remains unchanged (or invariant) under some transformation. In this case, we consider the transformation that interchanges the roots of $p(x)$. Such an interchange takes $r - s$ to $s - r$, but $\Delta = (r - s)^2 = (s - r)^2$, so the value of Δ remains unchanged.