Math 4030-001/Foundations of Algebra/Fall 2017

Polynomials at the Foundations: Roots

Next, we turn to the notion of a **root** of a polynomial in $\mathbb{Q}[x]$.

Definition 8.1. $r \in \mathbb{Q}$ is a **rational root** of $f(x) \in \mathbb{Q}[x]$ if $f(r) = 0$.

Examples. (a) The (non-zero) constant polynomials have no roots.

(b) Every linear polynomial has one rational root.

$$sx + t = 0; \quad r = -t/s$$

As a very easy consequence of division with remainders, we have:

Proposition 8.2. r is a root of $f(x)$ if and only if $x - r$ divides $f(x)$.

Proof. If $x - r$ divides $f(x)$, then:

$$f(x) = (x - r)q(x) \text{ and } f(r) = (r - r) \cdot q(r) = 0$$

so r is a root. On the other hand, if $x - r$ does not divide $f(x)$, then:

$$f(x) = (x - r)q(x) + s \text{ and } f(r) = (r - r)q(r) + s = s$$

for some non-zero constant (remainder term) s, so r is not a root. $\square$

Corollary 8.3. If $\deg(f(x)) = d$, then $f(x)$ has **at most** d roots.

Proof. Let $r_1, ..., r_n$ be **different** roots of $f(x)$. Then:

$$f(x) = (x - r_1)f_1(x)$$

and $r_2, ..., r_n$ are roots of $f_1(x)$ (they are not roots of $x - r_1$!), so:

$$f(x) = (x - r_1)f_1(x) = (x - r_1)(x - r_2)f_2(x)$$

and $r_3, ..., r_n$ are roots of $f_2(x)$. Eventually,

$$f(x) = (x - r_1) \cdots (x - r_n)f_n(x)$$

and then taking degrees, we get: $\deg(f_n(x)) + n = d$, so $n \le d$. $\square$

We can put polynomials $f(x) \in \mathbb{Q}[x]$ in a convenient form without changing their roots. If all the coefficients of $f(x)$ are in lowest terms:

$$f(x) = \frac{a_d}{n_d}x^d + \cdots + \frac{a_0}{n_0}$$

multiply through by the *least common multiple* of the denominators to get a polynomial with integer coefficients and no common factors.

Definition 8.4. A polynomial $f(x) \in \mathbb{Q}[x]$ with integer coefficients that share no common factor is in **lowest terms**. If we additionally require that such a polynomial have a positive leading term, then the lowest terms of a polynomial $f(x) \in \mathbb{Q}[x]$ is unique.

Example. The polynomial $\frac{1}{2}x^2 - \frac{2}{3}x + \frac{3}{4}$ times 12 is:

$$6x^2 - 8x + 9$$

which is in lowest terms, despite the fact that several **pairs** of the coefficients share prime factors.

Proposition 8.5. Let $f(x) = a_d x^d + \cdots + a_0$ be given in lowest terms. If $r = a/n$ is a root of $f(x)$, then n divides a_d and a divides a_0.

Proof. If a/n is a root, then:

$$f(r) = a_d \left(\frac{a}{n}\right)^d + \cdots + a_0 = 0$$

Multiplying through by n^d, gives:

$$a_d a^d + a_{d-1} a^{d-1} n + \cdots a_1 a n^{d-1} + a_0 n^d = 0$$

and if we isolate the first term and last term separately, we get:

$$a_d a^d + n\left(a_{d-1}a^{d-1} + \cdots + a_0 n^{d-1}\right) = 0 \text{ and}$$
$$a\left(a_d a^{d-1} + \cdots + a_1 n^{d-1}\right) + a_0 n^d = 0$$

But since a and n are relatively prime and: $n | a_0 a^d$ and $a | a_d n^d$, from the two equations, we get $n | a_0$ and $a | a_d$ as desired.

This Proposition gives us the **Rational Roots Test:**

To detect whether $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Q}[x]$ (in lowest terms) has a rational root, it suffices to check all the rational numbers:

$$\frac{a}{n}$$

where a divides a_0 and n divides a_d.

Examples. (a) For polynomials of the form:

$$f(x) = x^d - b$$

the only rational roots are integers dividing b. In other words, the only way that b has a dth root as a rational number is if it has a dth root as an integer! This gives another proof that 2 has no rational square root (or any dth root), since $1, -1, 2, -2$ are clearly not dth roots of 2.

(b) For quadratic polynomials $ax^2 + bx + c$ in lowest terms, the quadratic equation seems to contradict the rational roots test!

The formula:

$$r = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

suggests that the rational roots have denominator $2a$, which does not divide the leading coefficient! But the contradiction is resolved if we look more closely at the situation. By Example (a), if $\sqrt{b^2 - 4ac}$ is rational, then it is an integer. If b is even, then $\sqrt{b^2-4ac}$ is divisible by 4, and the overall numerator is even. If b is odd, then $\sqrt{b^2-4ac}$ is odd, and the numerator is once again even. Thus the quadratic formula produces a fraction that is not in lowest terms, and the contradiction is resolved by dividing numerator and denominator by 2.

Example. Applying the quadratic formula to $3x^2-x-4$ gives:

$$r = \frac{1 \pm \sqrt{1-(-48)}}{6} = \left\{ \frac{1+7}{6} = \frac{4}{3} \text{ and } \frac{1-7}{6} = -1 \right\}$$

Suppose, however, that the rational roots test fails?

Question. What are the "roots" when there are no rational roots?

There are several answers to this. One is to complete the rational numbers using analysis to the real numbers, and then to the complex numbers by "adjoining" i, in which case one can (and we will) prove:

The Fundamental Theorem. Every polynomial has a complex root.

But this does not tell us what the roots are. The strength of the quadratic formula is that it explicitly gives us the roots in terms of square roots of rational numbers. There is a similar explicit formula for cubic polynomials, which we will give below, and for fourth degree polynomials, which we will explore later. But there is no such formula for roots of polynomials of degree five or more! This requires thinking abstractly about roots, and is the foundation of "modern" algebra.

Recall the proof of the **Quadratic Formula.** To find roots of:

$$ax^2+bx+c=0$$

(i) Divide by a and rename the coefficients $p=b/a$ and $q=c/a$.

$$x^2+px+q=0$$

(ii) Use $\left(x+\frac{p}{2}\right)^2 = (x^2+px)+\frac{p^2}{4}$ and substitute for x^2+px:

$$(x^2+px)+q = \left(\left(x+\frac{p}{2}\right)^2 - \frac{p^2}{4}\right)+q=0$$

(iii) Rename $y=x+\frac{p}{2}$ and solve:

$$y^2 = -q+\frac{p^2}{4} \quad \text{and} \quad y=\pm\sqrt{-q+\left(\frac{p}{2}\right)^2}$$

and then substitute back:

$$x = y-\frac{p}{2} = -\frac{p}{2} \pm \sqrt{-q+\left(\frac{p}{2}\right)^2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

We initially approach a cubic polynomial in the same way:

The Cubic Formula: To find the roots of:

$$ax^3 + bx^2 + cx + d = 0$$

(i) Divide by a and rename: $r = b/a, s = c/a, t = d/a$:

$$\left(x^3 + rx^2\right) + sx + t = 0$$

(ii) Use $(x + r/3)^3 = x^3 + rx^2 + (r^2/3)x + (r^3/27)$ and substitute:

$$\begin{aligned} \left(\left(x + \tfrac{r}{3}\right)^3 - \left(\tfrac{r^2}{3}\right)x - \left(\tfrac{r^3}{27}\right)\right) + sx + t &= \\ \left(x + \tfrac{r}{3}\right)^3 + \left(s - \tfrac{r^2}{3}\right)x + \left(t - \tfrac{r^3}{27}\right) &= 0 \end{aligned}$$

(iii) Rename $y = x + \frac{r}{3}$:

$$\begin{aligned} y^3 + \left(s - \tfrac{r^2}{3}\right)\left(y - \tfrac{r}{3}\right) + \left(t - \tfrac{r^3}{27}\right) &= \\ y^3 + \left(s - \tfrac{r^2}{3}\right)y + \left(t - \left(\tfrac{r}{3}\right)s + \tfrac{2r^3}{27}\right) &= 0 \end{aligned}$$

(iv) Rename $p = s - \frac{r^2}{3}$ and $q = t - \frac{r}{3}s + \frac{2r^3}{27}$ to get:

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

But now how do we proceed? By an extraordinary change of variables!

$$y = z - \frac{p}{3z}$$

$$\begin{aligned} 0 &= \left(z - \tfrac{p}{3z}\right)^3 + p\left(z - \tfrac{p}{3z}\right) + q \\ &= \left(z^3 - zp + \tfrac{p^2}{3z} - \tfrac{p^3}{27z^3}\right) + \left(pz - \tfrac{p^2}{3z}\right) + q \\ &= z^3 - \tfrac{p^3}{27z^3} + q \\ &= \left(\tfrac{1}{z^3}\right)\left(z^6 + qz^3 - \tfrac{1}{27}p^3\right) \end{aligned}$$

(iv) Solve with the quadratic formula (assuming $z \neq 0$).

$$z^3 = \frac{-q \pm \sqrt{q^2 + \frac{4}{27}p^3}}{2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

and then substitute back for y:

$$y = z - \frac{p}{3z} = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}}$$

When we rationalize the denominator on the right, we get a surprise:

$$\frac{1}{\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}}\,\frac{\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}}{\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}}=\frac{\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}}{-\frac{p}{3}}$$

and so, finally, we get:

$$(*)\quad y=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

And you can in principle substitute all the way back to a, b, c, d to get a very ugly but explicit analogue of the quadratic formula.

Examples. (a) y^3+6y+2. ($p=6$ and $q=2$)

$$y=\sqrt[3]{-1+3}+\sqrt[3]{-1-3}=\sqrt[3]{2}-\sqrt[3]{4}$$

(b) y^3-7y-6. This looks pretty bad:

$$y=\sqrt[3]{3+\sqrt{-\frac{100}{27}}}+\sqrt[3]{3-\sqrt{-\frac{100}{27}}}$$

but the roots are $-1, -2$ and 3. All three are rational, and yet the cubic formula requires taking the square root of a negative number!

Remark. We will look into this more closely when we have the complex numbers, and then again when we think about the symmetries of roots. In particular, you should be worried in the final formula about which cube roots we are taking for each of the pair of terms.

Exercises. 8.1. Find quartic (degree four) polynomials in $\mathbb{Q}[x]$ with $0, 1$ and 2 rational roots, but show that there is no quartic polynomial with exactly 3 rational roots and one irrational root.

8.2. Given x^3+px+q, suppose that:

$$\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3=0$$

Show that $q/2$ has a **rational** cube root r and that

$$y^3+py+q=(x-2r)(x+r)^2$$

8.3. Try to make sense out of the the cubic formula when:

(a) $p=0$ (b) $q=0$.

Notice that in these two cases you know what the roots are!

8.4. Find a formula for the roots of $x^4+px^2+q=0$.