Math 222: Cubic Equations and Algebraic Expressions

Example. We claimed in class that none of the solutions to the equation $8x^3 - 6x - 1 = 0$ ha a degree two algebraic expression in the integers, $\mathbb{Z}$ . . . from which we concluded that one could not trisect an arbitrary angle with ruler and compass. How would one rigorously prove this claim about the solutions?

Let's step back a bit. Consider quadratic equations: $ax^2 + bx + c = 0$, where the coefficients $a, b, c \in \mathbb{Z}$. We know that every solution is degree two algebraic in $\mathbb{Z}$ - via the quadratic formula. But, sometimes the expression is *rational* in $\mathbb{Z}$. That is we don't need to take a square root. For example, $x^2 - 4 = 0$ clearly has solutions $x = \pm 2$.

Note: A number has a rational expression in the integers precisely if it is a rational number, i.e. a quotient of integers.

Question: Is there a way to "characterize" when the solutions are actually rational?

Answer: Yes! The point is that we can always **factor** the quadratic. e.g. $x^2 - 4 = (x-2)(x+2)$ or $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$. What is different about these two factorizations? In the first case, the factors are linear polynomials with rational (in fact integer) coefficients, whereas in the second case, the coefficients are not all rational numbers (e.g. $\sqrt{2}$ is not a rational number. In summary, can you prove the following fact?

Proposition 1. The solutions to a quadratic equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{Z}$ are rational if and only if $ax^2 + bx + c$ factors as $(dx + e)(fx + g)$ where each of d, e, f, g are rational numbers.

Question: Do you think a similar sort of result holds for cubic polynomials?

The answer is again yes, but life is a little more complicated. From Section 3.1, we now know that the solutions to any cubic (with integer coefficients) have degree three algebraic expressions in the integers. However, they might be rational or degree two algebraic in the integers. How do we tell what happens? Well, this is more complicated to prove, but what turns out to be true is the following.

Proposition 2. The solutions to a cubic equation $ax^3 + bx^2 + cx + d = 0$ with $a, b, c, d, \in \mathbb{Z}$ are all degree two algebraic in the integers if and only if the polynomial factors as
$(ex + f)(gx^2 + hx + j)$ for some rational numbers e, f, g, h, j.

Question. What is the condition for all the solutions to in fact be rational numbers?

Example. We have seen that the cube roots of unity in fact have degree two algebraic expressions in $\mathbb{Z}$. Of course, these are solutions to the equation $x^3 - 1 = 0$. Notice that $x^3 - 1 = (x - 1)(x^2 + x + 1)$. The first factor has solution $x = 1$ of course, and the solutions of the second factor are precisely ω and ω^2.

Example. Let's return now to our original example of $8x^3 - 6x - 1 = 0$. We want to show that the solutions are not degree two algebraic in $\mathbb{Z}$. ¿From Proposition 2, it suffices to show that the polynomial does not factor over the rational numbers. Hmm... how to do this. The key is to notice that if it factors, then one of the factors is of the form $ex + f$ and so one solution is $x = -f/e$, a rational number!! Hence, all the solutions will be degree two algebraic in $\mathbb{Z}$ if and only if at least one of the solutions is a rational number.

Now, how can we figure out if that is so or not? Obviously we can't check every rational number. Well, there is a very beautiful little fact which narrows things down for us. Indeed, you may have seen this before.

Proposition 3 - Eisenstein's Criterion. Let $ax^3+bx^2+cx+d=0$ be a cubic equation with $a,b,c,d\in\mathbb{Z}$ (with $a\neq 0$). Suppose that $x=\frac{u}{v}$ is a rational solution. That is $u,v\in\mathbb{Z}$. Assume further that the fraction is reduced so that u and v have no common factors. Then u must divide d and v must divide a.

Proof. We are assuming that $\frac{u}{v}$ is a solution so

$$a\left(\frac{u}{v}\right)^3+b\left(\frac{u}{v}\right)^2+c\left(\frac{u}{v}\right)+d=0.$$

Multiplying through by v^3 (notice that $v\neq 0$), we get

$$au^3+bu^2v+cuv^2+dv^3=0.$$

By appropriate subtractions and factoring, we get

$$(1)\qquad au^3=-(bu^2v+cuv^2+dv^3)=-(bu^2+cu^2v+dv^2)v$$

and

$$(2)\qquad u(au^2+buv+cv^2)=au^3+bu^2v+cuv^2=-dv^3.$$

¿From (1) we see that v must divide au^3, but u and v have no common factors so v must divide a. Similarly, from (2) we see that u must divide dv^3, and so u must divide d as claimed.

Note. This fact holds for polynomials of any degree. Can you state what's true in general?

Example. Let's apply Eisenstein's Criterion to the equation $8x^3-6x-1=0$. Here $a=8$ and $d=-1$. If a rational number u/v is a solution, then u must divide -1, so $u=\pm1$. And v must divide 8, so $v=\pm1,\pm2,\pm4,\pm8$. In summary, the only rational numbers which could possibly be solutions are $\pm1,\pm\frac{1}{2},\pm\frac{1}{4},\pm\frac{1}{8}$. Now, one just explicitly checks that none of these eight possibilities works. Hence the polynomial does not factor over the rationals and so none of the solutions can be degree two algebraic over $\mathbb{Z}$.

Final Thoughts: You may or may not have noticed a variety of subtleties in the above discussion about factoring polynomials. Factoring polynomials is something we will discuss in more detail later in the semester. One point to note for now is that when factoring, one has to be very clear about the world in which one is living, i.e. what sort of numbers (integers, rational, real, complex ??) you allow as coefficients when you factor.

Final Question: Is there a similar characterization in terms of factoring for higher degree polynomials? Notice that the solutions to $x^4-2=0$ are all degree two algebraic in $\mathbb{Z}$, but this does not factor into quadratics over the rational numbers.