Math Club Notes: 2007 March 7

1 Fields pin coefficients

Previously, in math club:

Definition 1 Let R be a subring of $\mathbb{R}$, and let p be a polynomial with coefficients in $\mathbb{R}$. We say that p *fixes* R if $p(t) \in R$ for all $t \in R$.

Definition 2 Let R be a subring of $\mathbb{R}$. We say that R *pins coefficients* if every polynomial which has real coefficients and fixes R must have coefficients which are all in R.

On January 24 we observed that $\mathbb{Z}$ doesn't pin coefficients; for example, $\frac{1}{2}t(t+1)$ fixes $\mathbb{Z}$ but has coefficients not in $\mathbb{Z}$.

On February 28 we observed that any ring is fixed by the identity polynomial $p(t) = t$, and so any ring that pins coefficients must contain 1; by closure under addition, any ring that pins coefficients must contain all of $\mathbb{Z}$.

Today we looked at a proof that $\mathbb{Q}$ pins coefficients.

Let $r_0, r_1, \ldots, r_n$ be some $n+1$ distinct rational numbers, and consider the matrix

$$M = \begin{bmatrix} 1 & r_0 & r_0^2 & \ldots & r_0^n \\ 1 & r_1 & r_1^2 & \ldots & r_1^n \\ 1 & r_2 & r_2^2 & \ldots & r_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & r_n & r_n^2 & \ldots & r_n^n \end{bmatrix}.$$

Note that if p is the polynomial

$$p(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

then

$$M \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} p(r_0) \\ p(r_1) \\ p(r_2) \\ \vdots \\ p(r_n) \end{bmatrix}.$$

In particular, any solution to the homogeneous system $Mx = 0$ gives rise to a polynomial p such that $p(r_0) = p(r_1) = \cdots = p(r_n) = 0$. Since the r_i are distinct, that means p has $n+1$ roots; but it has degree at most n. So if p corresponds to a solution to $Mx = 0$, then p is the zero polynomial, and so all the components of x are zero.

In other words: the homogeneous system $Mx = 0$ has only the trivial solution. That is, M is invertible.

(We've just shown that if the r_i are distinct, then M is invertible. The converse is also true: if some two of the r_i are equal, then two rows of M are equal, so M's rows are linearly dependent.)

Now we can prove that $\mathbb{Q}$ pins coefficients. Let p be a polynomial which fixes $\mathbb{Q}$. Let x be the vector corresponding to p, as above. Then, as above, the ith component of Mx is $p(r_i)$. Since all the r_i are rational, and p fixes $\mathbb{Q}$, all the $p(r_i)$ are rational. And since all the entries of M are rational, all the entries of M^{-1} are rational. Thus

$$x = M^{-1} \begin{bmatrix} p(r_0) \\ \vdots \\ p(r_n) \end{bmatrix}$$

also has rational components. That is, the coefficients of p are rational, which completes the proof.

This argument relies on only two properties of $\mathbb{Q}$: first, that it's infinite (so it has at least $n+1$ distinct elements); second, that if an invertible matrix has rational entries then its inverse also has rational entries. Any subfield of $\mathbb{R}$ has these properties, so we've actually shown the result for any such field.

So far, then, we know that all fields in $\mathbb{R}$ fix coefficients, and that any ring in $\mathbb{R}$ that fixes coefficients must contain $\mathbb{Z}$ as a proper subring. We still don't know whether there are any rings that fix coefficients but are not fields.

2 A weird problem from Barbeau

Another problem from our list (Barbeau's problem 1.8.4): Let p be a monic quadratic polynomial with integer coefficients. Show that, for every integer n, there exists an integer k such that $p(n)p(n+1) = p(k)$.

The natural thing to try is to let

$$p(t) = t^2 + bt + c$$

and just write it all out: we want to find k in terms of n so that

$$(n^2 + bn + c)((n+1)^2 + b(n+1) + c) = k^2 + bk + c \ .$$

Now, you could multiply out the LHS and try to bang it into the shape of the RHS, but... well, it doesn't look like a lot of fun.

It's a little better to solve this problem by considering some special cases. Let's take $p(t) = t^2$, the simplest monic quadratic polynomial. We wish to find k in terms of n so that

$$n^2(n+1)^2 = k^2 \ ,$$

and obviously $k = n(n+1)$ will do.

Let's try $p(t) = t^2 + 1$. We want k so that

$$(n^2 + 1)(n^2 + 2n + 2) = k^2 + 1 ,$$

that is, multiplying out and rearranging,

$$k = \sqrt{n^4 + 2n^3 + 3n^2 + 2n + 1} = n^2 + n + 1 .$$

With a little luck we notice that in both cases we have $k = p(n)+n$. Proving that this works is routine.

Much more interesting, though, is Barbeau's solution. Let, he says,

$$q(t) = p(n + t) .$$

q is a polynomial, since it is a composition of polynomials. Moreover, q is a composition of a linear and a quadratic polynomial, both monic; so q is a monic quadratic polynomial. Let

$$q(t) = t^2 + bt + c .$$

Then

$$p(n)p(n + 1) = q(0)q(1) = c(1 + b + c) = c^2 + bc + c = q(c) = p(n + c) ,$$

and so obviously we can take $k = n + c$.

Nifty, eh?

I suspect this idea — to notice the similarity of structure between two expressions (here, between $p(n) = p(n + 0)$ and $p(n + 1)$) and to turn the point where they differ into a parameter — to recur in other problems.