Math Club Notes: 2007 May 30

1 Polynomials that commute with squaring

One of our outstanding problems:[1] Find all polynomials which commute under composition with t^2, that is, find all polynomials f such that $f(t^2) = (f(t))^2$ for all t.

We first considered such f of low degree.

If f is constant, say $f(t) = a$, then $a^2 = a$, that is, $a = 0$ or $a = 1$.

If f is of degree 1, say $f(t) = at + b$ with $a \neq 0$, then

$$at^2 + b = f(t^2) = (f(t))^2 = a^2t^2 + 2abt + b^2 .$$

Identifying the coefficients of t^2 yields $a = 1$ (since $a \neq 0$); identifying the coefficients of t yields $ab = 0$, which since $a = 1$ entails $b = 0$; and that, happily, makes the constant coefficients equal too. So the only such polynomial of degree 1 is $f(t) = t$.

If f is of degree 2, say $f(t) = at^2 + bt + c$ with $a \neq 0$, then... well, I'll skip the details, but a similar argument yields $a = 1$, $b = 0$, and $c = 0$, so the only such polynomial of degree 2 is $f(t) = t^2$.

It's easy to become convinced at this point that the only such polynomials are the zero polynomial and the power functions: $0, 1, t, t^2, t^3, \ldots$.

Here's the beginning of a proof.

First note that if f is such a polynomial, then $f(0) = f(0^2) = (f(0))^2$, so that either $f(0) = 0$ or $f(0) = 1$.

If $f(0) = 0$, then t divides $f(t)$, that is, $f(t) = tg(t)$ for some polynomial g. Then g also has the desired property, since $t^2g(t^2) = f(t^2) = (f(t))^2 = t^2(g(t))^2$. Apply the same argument to g iteratively.

Either we can divide by t forever, in which case f is the zero polynomial, or eventually we obtain $f(t) = t^n g(t)$ with $g(0) = 1$. Let

$$g(t) = \sum_{k\geq 0} a_k t^k ,$$

where $a_0 = 1$. We wish to show that $a_k = 0$ for all $k \geq 1$ (so that $g(t) = 1$ and $f(t) = t^n$). By hypothesis, $g(t^2) = (g(t))^2$, so

$$\sum_{k\geq 0} a_k t^{2k} = \left(\sum_{k\geq 0} a_k t^k\right)^2 = \sum_{k\geq 0}\sum_{j\geq 0} a_k a_j t^{k+j} = \sum_{\ell\geq 0}\left(\sum_{k=0}^{\ell} a_k a_{\ell-k}\right)t^\ell .$$

Now identify coefficients of like powers of t and prove by induction on k that $a_k = 0$ for all $k \geq 1$.

[1] E.J. Barbeau, *Polynomials* (Springer, 1989), exercise 1.1.21.

2 A trigonometric inequality, two ways

The problem: prove[2] that, in triangle $\triangle ABC$,

$$\sin\frac{A}{2} \le \frac{a}{b+c}\,.$$

(As per the usual convention, a, b, and c are the (lengths of the) sides opposite the angles A, B, and C respectively.)

2.1 First solution

The solution given by Andreescu and Feng goes something like this:

$$\begin{aligned}
\frac{a}{b+c} &= \frac{\sin A}{\sin B + \sin C} && \text{(law of sines)}\\
&= \frac{2\sin\frac{A}{2}\cos\frac{A}{2}}{\sin B + \sin C} && \text{(double-angle identity)}\\
&= \frac{2\sin\frac{A}{2}\cos\frac{A}{2}}{2\sin\frac{B+C}{2}\cos\frac{B-C}{2}} && \text{(sum-to-product identity)}\\
&= \frac{2\sin\frac{A}{2}\cos\frac{A}{2}}{2\sin\frac{180^\circ-A}{2}\cos\frac{B-C}{2}} && \text{(it's a triangle)}\\
&= \frac{2\sin\frac{A}{2}\cos\frac{A}{2}}{2\sin(90^\circ-\frac{A}{2})\cos\frac{B-C}{2}}\\
&= \frac{2\sin\frac{A}{2}\cos\frac{A}{2}}{2\cos\frac{A}{2}\cos\frac{B-C}{2}}\\
&= \frac{\sin\frac{A}{2}}{\cos\frac{B-C}{2}}\\
&\ge \sin\frac{A}{2} && \text{(since } \cos x \le 1\text{)}
\end{aligned}$$

For free, we get that there's equality just when $B = C$, that is, the triangle is isosceles with vertex A.

The first couple steps are quite natural: the inequality relates sines of angles to lengths of sides, so we use the law of sines; we then have $\sin A$ and want $\sin\frac{A}{2}$, so we use the double-angle identity. I think you'd only think to use the sum-to-product identity in the next step if you could see ahead a couple steps and anticipate some cancellations.

This is the kind of solution you come up with if you already know what you're trying to prove (and know your trig identities); the next solution is, perhaps, a more likely way to discover the inequality.

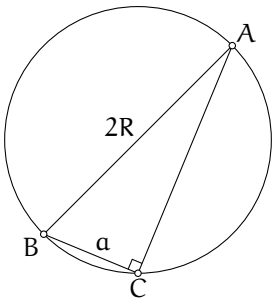
[2] Titu Andreescu and Zuming Feng, *103 Trigonometry Problems* (Boston: Birkhäuser, 2005), introductory problem #8.

2.2 Second solution

The first ingredient is what they call the "extended" law of sines:

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R\,,$$

where R is the radius of the circle circumscribed around $\triangle ABC$. Note that if we fix B and C but move vertex A along the arc it's on, then the size of angle A doesn't change[3] and of course the length of side a doesn't change either. Thus $a/\sin A$ is constant as A varies along that arc.

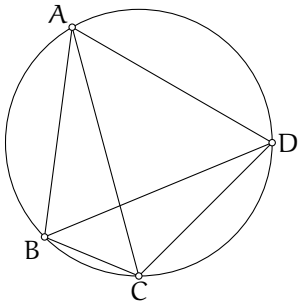


If we place A so that AB is a diameter of the circle, then $C = 90°$ (Thales' theorem), and we can read off that $\sin A = a/2R$. The extended law of sines follows.

(Well, we have to consider the case when A is on the other side of the chord BC, where it cannot be placed to make AB a diameter. I'll leave this to you.)

The second ingredient is Ptolemy's theorem: if $ABCD$ is a simple cyclic quadrilateral, then

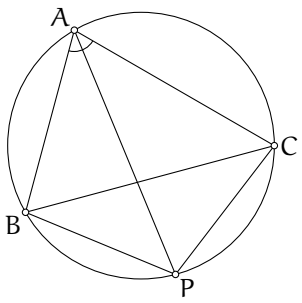
$$|AC||BD| = |AB||CD| + |AD||BC|$$



That is, the product of the diagonals is the sum of the products of the opposite sides.

[3] Euclid III:21. See http://www.amotlpaa.org/math/iii21.html for an animated illustration.

Now, suppose we have some triangle $\triangle ABC$ (with its circumcircle), and we bisect angle A and extend the bisector to intersect the circumcircle[4] at, say, P.



By Ptolemy's theorem,

$$|AP||BC| = |AC||BP| + |AB||CP| .$$

By the extended law of sines (for $\triangle ABP$), $|BP| = 2R \sin \frac{A}{2}$; likewise, $|CP| = 2R \sin \frac{A}{2}$. Thus we have

$$|AP||BC| = 2R(|AC| + |AB|) \sin \frac{A}{2} .$$

BC, AC, and AB are sides of $\triangle ABC$, and their lengths are by convention a, b, c respectively; using those names, we have

$$|AP|a = 2R(b + c) \sin \frac{A}{2} .$$

Rearranging,

$$\frac{a}{b + c} = \frac{2R}{|AP|} \sin \frac{A}{2} .$$

The inequality then follows since $2R$ is the diameter of the circumcircle and $|AP|$ is a chord in it.

Again, the proof yields a condition for having equality: when the bisector of angle A is a diameter of the circumcircle. (It is easy to verify that this condition is equivalent to the one we had before.)

These two solutions are actually not as different as they might appear; the combination of Ptolemy's theorem and the law of sines is essentially the addition identity for sine, which in this case (since we're bisecting the angle) reduces to the double-angle identity used in the first solution.

[4] See http://www.amotlpaa.org/math/incentre.pdf for a nifty result about this situation.

3 A telescoping trigonometric product

A new problem:[5] to show that

$$\cos 20^\circ \cos 40^\circ \cos 80^\circ = \frac{1}{8} .$$

Seeing the sequence $20, 40, 80$, we naturally think of the double-angle identities. Or rather, we naturally think of the double-angle identity for cos; but it turns out what we need is the double-angle identity for sin:

$$\sin(2\theta) = 2 \sin\theta \cos\theta .$$

Thus

$$\cos 20^\circ \cos 40^\circ \cos 80^\circ = \frac{\sin 40^\circ}{2 \sin 20^\circ} \cdot \frac{\sin 80^\circ}{2 \sin 40^\circ} \cdot \frac{\sin 160^\circ}{2 \sin 80^\circ} = \frac{\sin 160^\circ}{8 \sin 20^\circ} = \frac{1}{8} ,$$

the last step since $\sin 160^\circ = \sin(180^\circ - 20^\circ) = \sin 20^\circ$.

(This way to use the double-angle identity for sine to make a telescoping product was mentioned in our notes for 2005 March 22.)

By the way, it's conceivable to approach the problem by computing the three cosines directly. A traditional method: if $x = n\pi/9$ (where $n \in \mathbb{Z}$), then $\sin(9x) = 0$, and so

$$\begin{aligned} 0 &= \operatorname{Im}(\cos(9x) + i \sin(9x)) \\ &= \operatorname{Im}(\cos x + i \sin x)^9 \\ &= \operatorname{Im}(\cos^9 x + 9i \cos^8 x \sin x - 36 \cos^7 x \sin^2 x - 84i \cos^6 x \sin^3 x + \cdots) \\ &= 9 \cos^8 x \sin x - 84 \cos^6 x \sin^3 x + \cdots \end{aligned}$$

In this last expression, cos occurs only in even powers, which can be converted to sin with the Pythagorean identity; this yields a polynomial of degree 9 in $\sin x$. In fact, all the powers of sin are odd, so we can divide out one $\sin x$ to get a polynomial of degree 4 in $\sin^2 x$. The zeroes of that polynomial are, then, the values $\sin^2(n\pi/9)$.

Quartics are solvable (though hardly anybody actually knows the method off the top of their head), so in principle you can find the value of $\sin(\pi/9) = \sin 20^\circ$ this way, then use that to find the values in the question. It looks like a lot of work, though.

(This is, however, a good way to find the values of $\sin(\pi/5)$ and $\cos(\pi/5)$; we've all been taught the values of trig functions at π, $\pi/2$, $\pi/3$, $\pi/4$, and $\pi/6$, and the $\pi/5$ values fill in that list nicely.)

[5] I read about this problem in Beyer, Louck and Zeilberger, "A generalization of a curiosity that Feynman remembered all his life", *Mathematics Magazine* 69(1) (February 1996), 43–44 (also at http://www.math.temple.edu/~zeilberg/mamarim/mamarimhtml/feynman.html; they quote a Feynman anecdote from p. 47 of James Gleick's book *Genius*.

4 An arcsin identity

The identity:

$$2\arcsin\sqrt{\frac{x}{2}} - \arcsin(x-1) = \frac{\pi}{2}\,.$$

For the LHS to be defined we require that $x \in [0,2]$. Rearranging, we wish to show

$$2\arcsin\sqrt{\frac{x}{2}} = \frac{\pi}{2} + \arcsin(x-1)\,.$$

Both LHS and RHS here are in $[0,\pi]$; on this interval cos is one-to-one, so the equality is equivalent to

$$\cos\left(2\arcsin\sqrt{\frac{x}{2}}\right) = \cos\left(\frac{\pi}{2} + \arcsin(x-1)\right)\,,$$

which by a couple identities is equivalent to

$$1 - 2\sin^2\arcsin\sqrt{\frac{x}{2}} = -\sin\arcsin(x-1)\,,$$

that is,

$$1 - x = -(x-1)\,,$$

which of course is true.

The origin of this problem is a calculus exam question that Dr. Litvak mentioned to me, more or less to evaluate

$$\int \frac{1}{\sqrt{2x-x^2}}\,dx\,.$$

The traditional method is to complete the square and apply a trig substitution:

$$\begin{aligned}
\int \frac{1}{\sqrt{2x-x^2}}\,dx &= \int \frac{1}{\sqrt{1-(1-x)^2}}\,dx \\
&= -\int \frac{1}{\sqrt{1-u^2}}\,du && (u = 1-x) \\
&= -\int \frac{1}{\sqrt{1-\sin^2 t}}\cos t\,dt && (u = \sin t;\ t \in [-\tfrac{\pi}{2}, \tfrac{\pi}{2}]) \\
&= -\int \frac{1}{\cos t}\cos t\,dt && (\cos t \geq 0 \text{ for } t \in [-\tfrac{\pi}{2}, \tfrac{\pi}{2}]) \\
&= -\int dt \\
&= -t + C \\
&= \arcsin(x-1) + C\,.
\end{aligned}$$

One of his students, however, thought of the following:

$$\begin{aligned}
\int \frac{1}{\sqrt{2x - x^2}}\,dx &= 2\int \frac{1}{\sqrt{2-x}} \cdot \frac{1}{2\sqrt{x}}\,dx \\
&= 2\int \frac{1}{\sqrt{2-u^2}}\,du \qquad\qquad (u = \sqrt{x}) \\
&= 2\int \frac{1}{\sqrt{1-(u/\sqrt{2})^2}} \cdot \frac{1}{\sqrt{2}}\,du \\
&= 2\arcsin\frac{u}{\sqrt{2}} + C \\
&= 2\arcsin\sqrt{\frac{x}{2}} + C\,.
\end{aligned}$$

If you're marking such an exam, naturally your first reaction to the second answer is that it must be wrong. But no; it turns out these two expressions differ by a constant.

(It's easy to find out what the constant is; just plug in $x = 0$, or $x = 1$.)

This background yields another approach to proving the identity: verify it holds at one value, and check that the derivative of the (original) LHS is zero.

5 More rings that don't pin coefficients

Previously, in math club:

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

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

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 $\mathbb{Z}$.

On March 7 we proved that every subfield of $\mathbb{R}$ pins coefficients. (So the remaining question is whether there exist any rings which are not fields but do pin coefficients.)

Before, we used the polynomial $\frac{1}{2}t(t+1)$ to show that $\mathbb{Z}$ doesn't pin coefficients. It's a little tidier to use

$$\frac{1}{2}t(t-1)$$

instead. What makes this work is that there are just two equivalence classes modulo 2 in $\mathbb{Z}$; everything is congruent modulo 2 either to 0 or to 1. Put another

way: for any integer t, either $t-0$ is even or $t-1$ is even. Thus their product is even for all integers t, and so $\frac{1}{2}(t-0)(t-1) \in \mathbb{Z}$ for all $t \in \mathbb{Z}$, which is exactly the statement that this polynomial fixes $\mathbb{Z}$. But its leading coefficient is, of course, the non-integer $\frac{1}{2}$.

A similar construction works in some other rings. For example, consider the equivalence classes modulo 2 in the ring

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\}.$$

It is easy to see that the multiples of 2 in this ring are just those $a + b\sqrt{2}$ for which a and b are even. So:

if a and b are both even,	then 2 divides $a + b\sqrt{2}$;
if a is even and b is odd,	then 2 divides $a + (b-1)\sqrt{2}$;
if a is odd and b is even,	then 2 divides $(a-1) + b\sqrt{2}$;
if a and b are both odd,	then 2 divides $(a-1) + (b-1)\sqrt{2}$.

Thus, for any $t \in \mathbb{Z}[\sqrt{2}]$, one of the numbers

$$t, \quad t-\sqrt{2}, \quad t-1, \quad t-1-\sqrt{2}$$

is a multiple of 2. So the polynomial

$$\frac{1}{2}t(t-\sqrt{2})(t-1)(t-1-\sqrt{2})$$

fixes $\mathbb{Z}[\sqrt{2}]$, despite having leading coefficient $\frac{1}{2} \notin \mathbb{Z}[\sqrt{2}]$.

So $\mathbb{Z}[\sqrt{2}]$ doesn't pin coefficients.

(Considering this ring's equivalence classes modulo $\sqrt{2}$ yields a simpler polynomial.)

For another example, consider the ring $\mathbb{Z}[\frac{1}{2}]\ldots$ well, I'm not sure that notation is standard. What I mean is the ring consisting of all linear combinations of powers of $\frac{1}{2}$ with coefficients from $\mathbb{Z}$. This ring can also be defined by

$$\mathbb{Z}[\tfrac{1}{2}] = \left\{ \frac{a}{2^n} \colon a, n \in \mathbb{Z} \text{ and } n \geq 0 \right\}.$$

It consists of all numbers with finite binary expansions.

It turns out that $\mathbb{Z}[\frac{1}{2}]$ has three equivalence classes modulo 3; everything is congruent to 0, to 1, or to 2. (This might surprise you; it certainly surprised me. Example: in this ring, $\frac{1}{2} \equiv 2 \pmod 3$, since $2 - \frac{1}{2} = \frac{3}{2} = 3 \cdot \frac{1}{2}$ is a multiple of 3.) Thus the polynomial $\frac{1}{3}t(t-1)(t-2)$ fixes this ring, despite having leading coefficient $\frac{1}{3} \notin \mathbb{Z}[\frac{1}{2}]$.

For general A (a subring of $\mathbb{R}$ but not a field), this construction goes like this: Pick an element $m \in A$ whose inverse is not in A. Let $\{r_1, r_2, \ldots, r_k\}$

be a complete system of equivalence class representatives for the relation of congruence modulo m on A. Then the polynomial

$$\frac{1}{m}(t - r_1)(t - t_2) \cdots (t - r_k)$$

fixes A but has leading coefficient $\frac{1}{m} \notin A$, so A doesn't pin coefficients.

The only way this construction can go wrong is if there are infinitely many equivalence classes modulo m in A; then the polynomial constructed has infinite degree and so isn't a polynomial.

In summary: if A contains an uninvertible element m such that there are finitely many equivalence classes modulo m in A, then A doesn't pin coefficients. Thus if A does pin coefficients, then every uninvertible element in it gives rise to infinitely many equivalence classes.

This seems like an extremely strong constraint on rings that pin coefficients. I can only think of one situation where an element in a ring gives rise to infinitely many equivalence classes: the element 0. (Being congruent modulo 0 means differing by a multiple of 0, which means differing by 0, which means being equal. So every element is in its own equivalence class modulo 0.) The natural conjecture, then, is that no such ring exists; in other words, that pinning coefficients is equivalent to being a field.

(Postscript: That conjecture didn't last long; see our notes for August 22 for an example of a ring satisfying this "extremely strong constraint".)