Strange Fact

Peter Freyd
pjf@upenn.edu

Given a set let M *be a permutation with just two orbits one of which is a fixed point. Let* A *be a transitive permutation (i.e. a permutation with just a single orbit) that commutes with* $\mathsf{M}^i\mathsf{A}\mathsf{M}^{-i}$ *each* i*.*

Then the set is finite and the number of its elements is a prime.

If we drop the condition that A *be transitive but retain just that it doesn't fix the fixed point of* M*, then the order of the set is still finite but it needn't be prime.* A*, is, however, fixed-point–free and of prime order and the order of the set has to be a prime power.*

Of course one way to obtain such a weird-looking result is to impose a condition that can't be satisfied on any set. So note that a converse holds: if a finite set is of prime-power order we may obtain examples of M and A by imposing a field structure on the set, taking $\mathsf{M}(x) = rx$ where r is a primitive element and $\mathsf{A}(x) = 1+x$.

Given a set with permutations M and A with the properties described above we will obtain the result by doing no less than constructing a field structure on the set. We'll do so by "reversing" the example. Take 0 to be the fixed point of M and take 1 to be $\mathsf{A}(0)$. We'll use the letter r to denote $\mathsf{M}(1)$ and impose a multiplicative structure so that $0x = 0$ and $r^ix = \mathsf{M}^i(x)$ (making it, therefore, a cyclic group to which an annihilator element has been adjoined).

Define addition by $0 + y = y$ and for $x \neq 0$ define $x + y = x\big(\mathsf{A}(x^{-1}y)\big)$. To see that this is a field, note first that for $x \neq 0$ we have $x + 0 = x\big(\mathsf{A}(x^{-1}0)\big) = x\big(\mathsf{A}(0)\big) = x1 = x$. Distributivity requires no conditions on A: using that multiplication is commutative we need show only that $x(y + z) = (xy) + (xz)$; if either x or y is zero then it's immediate; otherwise $x(y+z) = x\big(y(\mathsf{A}(y^{-1}z)\big)$ and $(xy) + (xz) = (xy)\big(\mathsf{A}\big((xy)^{-1}(xz)\big)\big)$ easily checked to be equal. For subtraction denfine -1 as $\mathsf{A}^{-1}(0)$ and verify that $1 + (-1) = 1\big(\mathsf{A}\big(1^{-1}(-1)\big)\big) = \mathsf{A}\big(\mathsf{A}^{-1}(0)\big) = 0$. Distributivity then yields

$$x + x(-1) = x\big(1 + (-1)\big) = x0 = 0.$$

We dispatch both the commutativity of addition and its associativity by proving $x+(y+z) = y+(x+z)$. (Commutativity can then be obtained by taking $z = 0$ and associativity easily follows: $x+(y+z) = x+(z+y) = z + (x + y) = (x + y) + z$.)

The equation $x+(y+z) = y+(x+z)$ is immediate if either x or y is zero. Otherwise we let $u = x^{-1}y$ and $v = x^{-1}z$; it clearly suffices to prove $1+(u+v) = u+(1+v)$ (multiply by x and use distributivity). This last equation translates to $\mathsf{A}\big(u\mathsf{A}(u^{-1}v)\big) = u\big(\mathsf{A}\big(u^{-1}(\mathsf{A}(v))\big)\big)$. Since $u \neq 0$ and M is transitive on the complement of $\{0\}$, there is a natural number i such that $uw = \mathsf{M}^i(w)$ for all w. Hence the last equation rewrites to $\mathsf{A}\big(\mathsf{M}^i\big(\mathsf{A}\big(\mathsf{M}^{-i}(v)\big)\big)\big) = \mathsf{M}^i\big(\mathsf{A}\big(\mathsf{M}^{-i}\big(\mathsf{A}(v)\big)\big)\big)$, that is, it is the condition that A commutes with $\mathsf{M}^i\mathsf{A}\mathsf{M}^{-i}$.

The multiplicative group of a field can not be infinite cyclic (it would have only one $\sqrt{1}$, hence its characteristic would be two and with no finite subfields other than $\{0, 1\}$; but $1+r$ would have to be a power of r, quite enough therefore, for the subfield it generates to be finite and with more than two elements). The additive group of a finite field is, of course, of prime-power order and when adding 1 yields a transitive permutation it has to be cyclic.

f

Available at `http://www.math.upenn.edu/~pjf/prime-power.pdf`