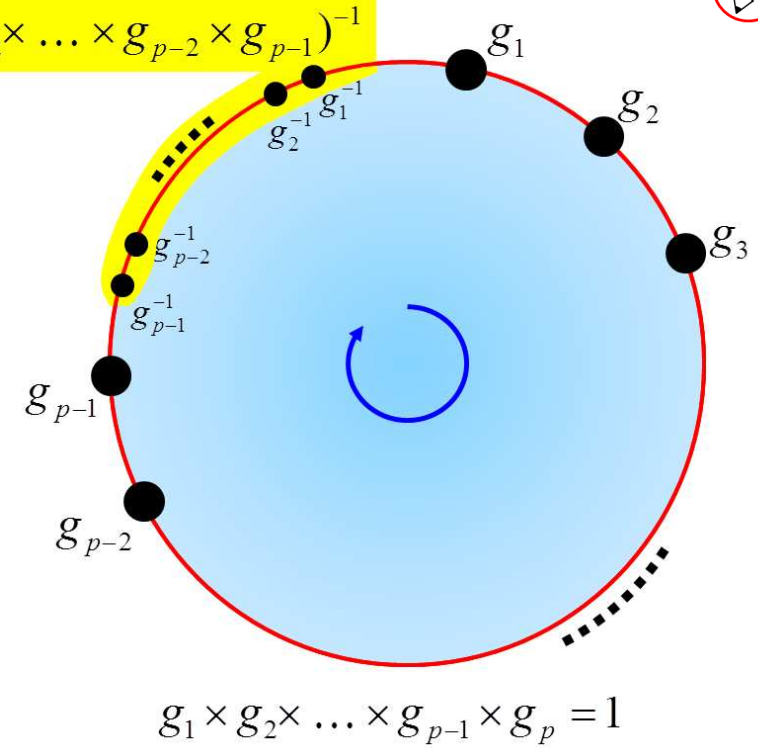
THEOREM OF THE DAY

Cauchy's Theorem in Group Theory *If the order of a finite group G is divisible by a prime p then G contains an element of order p.*

The multiplication table shown near right defines a group of order 10: there are 10 elements each appearing once in every row and column; one element, namely e (the **identity**) leaves everything unchanged by multiplication; and associativity holds so that, for example, $(t \times r) \times w = j \times w = e$ agrees with $t \times (r \times w) = t^2 = e$. We observe, meanwhile, that t is an element of order 2 (an *idempotent*, $t^2 = e$): Cauchy's theorem says such an element must exist since 2 divides 10. It is less immediate to confirm, but in fact, every non-identity element that is not an idempotent has order 5, the other prime dividing 10. And perhaps you have recognised the dihedral group D_{10}, in which case you know this already.*

×	e	t	r	d	j	a	w	s	k	i
e	e	t	r	d	j	a	w	s	k	i
t	t	e	j	k	r	i	s	w	d	a
r	r	w	e	s	a	j	t	d	i	k
d	d	a	k	j	w	s	i	r	t	e
j	j	s	t	w	i	r	e	k	a	d
a	a	d	w	t	k	e	r	i	j	s
w	w	r	a	i	e	k	d	t	s	j
s	s	j	i	a	t	d	k	e	w	r
k	k	i	d	r	s	w	a	j	e	t
i	i	k	s	e	d	t	j	a	r	w

$$g_p = (g_1 \times g_2 \times \ldots \times g_{p-2} \times g_{p-1})^{-1}$$



*You can recover the usual multiplication table of D_{10} by spotting that the group elements are an anagram of the name of a famous scientist.

Proof.

Denote by 1 the identity in an arbitrary finite group G of order, say, n. If p divides n then the number of solutions of $x^p = 1$ must in fact be a positive multiple of p. To see this, consider the set X_p of all ordered lists of p elements of G satisfying the identity: $g_1 g_2 \cdots g_{p-1} g_p = 1$. We can choose any values for $g_1, \ldots, g_{p-1}$, after which g_p is fixed; see the illustration above right. So $|X_p| = n^{p-1}$. Now for some lists in X_p all the g_i are identical. These correspond to the solutions to $x^p = 1$; suppose there are A such lists. Every other list has two properties: (1) it gives a different element of X_p if its elements are cycled round, because p is prime, so that a p-gon with non-identical vertices has no symmetries; and (2) if its elements are cycled round then they still multiply to 1, because g_p can be rewritten as $g_{p-1}^{-1} \cdots g_2^{-1} g_1^{-1}$ and cancellation of all elements will occur regardless of where we start multiplying (see the illustration). So the number, say B, of lists in X_p which do not give solutions to $x^p = 1$ is a multiple of p. And now since $A + B = n^{p-1}$ and B and n are both divisible by p, so must A be. And A is not zero, since 1 is a solution to $x^p = 1$, so A is a positive multiple of p.

Elements of order p generate subgroups of order p so Lagrange's Theorem, that a group's order must be divisible by that of any of its subgroups, has here a partial converse, greatly strengthened in Sylow's celebrated theorems of 1872. Cauchy proved his theorem (independently asserted without proof by Evariste Galois) in his seminal 1845 'Mémoire sur les arrangements que l'on peut former avec des lettres données'. The proof given above is due to James H. McKay, 1959.

Web link: qchu.wordpress.com/2013/07/09/

Further reading: *Topics in Group Theory* by Geoff Smith and Olga Tabachnikova, Springer, 2000, chapter 3.