



# THEOREM OF THE DAY

**Galois' Theorem on Finite Fields** *A finite field with  $n$  elements exists if and only if  $n = p^k$  for some prime  $p$  and some non-negative integer  $k$ . Moreover this field is unique up to isomorphism.*

$\times$	0	1	2	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	$x$	$x+2$	$x+1$
$x$	0	$x$	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	$x$
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	$x$	$x+1$	$2x$	2
$2x$	0	$2x$	$x$	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	$x$	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	$x$	2	$x+2$	1	$2x$

$+$	0	1	2	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	$x$	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	$x$	$x+1$	$2x+2$	$2x$	$2x+1$
$x$	$x$	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	$x$	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	$x$	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	$x$	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	$x$
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	$x$	$x+1$

A *field* is a collection of ‘numbers’ with addition and multiplication defined on it so as to behave analogously to the reals or rationals: there is a 0 for addition, a 1 for multiplication, you can divide consistently, etc. When the number of elements of the field is  $n$ , a non-negative integer, it is called *finite*. If  $n$  is a prime then addition and multiplication modulo  $p$  defines a field, denoted  $GF(p)$ . Thus in  $GF(3)$ ,  $2 \times 2 = 2 + 2 = 1$  since  $4 \pmod{3} = 1$ . But in, say  $GF(3^2)$ , modulo arithmetic on its own will not do, since  $3 \times 3 = 0 \pmod{9}$  and ‘properly behaved’ arithmetic should not give zero as the product of two nonzero numbers. Instead the ‘numbers’ of  $GF(p^k)$  are the polynomials of degree  $k - 1$  over  $GF(p)$ , with addition modulo  $p$  and multiplication defined using remainders modulo some chosen *irreducible polynomial*: one which cannot be written as a product of two polynomials of lower degree.

In the example above,  $GF(9)$  is constructed using the polynomial  $x^2 + 1$ , irreducible over  $GF(3)$ . Thus  $x^2$  can be written as  $(x^2 + 1) + 2$  modulo 3, so the remainder is 2 and, in  $GF(9)$ ,  $x^2 = 2$ . Now we can calculate, say,  $(2x + 1) \times (x + 2) = 2x^2 + 5x + 2 = 2 \times 2 + 5x + 2 = 5x + 6 = 2x$  modulo 3. The addition table is more easily calculated and divides naturally into regions, shown in colours here, which repeat according to the addition table of the base field  $p$ . By the way, in  $GF(9)$  this reminds one of a Sudoku puzzle, and one can indeed construct one. Replace  $x$  by 3 in the addition table. Add 0 to the first row of each  $3 \times 3$  block; add 3 to the second row; and add 6 to the final row. Take remainders modulo 9 and add 1. The result is a completed Sudoku.

The uniqueness of the finite field of order  $p^k$  is actually due to the American mathematician Eliakim Moore in 1893. Evariste Galois invented large parts of modern algebra, including finite field theory, before dying in a duel in 1832 at the age of 20. The great pianist Alfred Brendel has said he can forgive the early death of Franz Schubert “as little as I can forgive the death of Bücher, Masaccio or Keats, all of whom died even younger.” The loss of Galois, youngest of all, is surely no less unforgivable.

**Web link:** [designtheory.org/library/encyc/topics/gf.pdf](http://designtheory.org/library/encyc/topics/gf.pdf)

**Further reading:** *Galois Theory* by Ian Stewart, Chapman & Hall/CRC; 3Rev Ed, 2003. The Brendel quote is in *The Veil of Order*, Faber, 2002, p.122.

