Classification of Finite Fields

For each prime *p* and for each positive integer *n*, there is, up to isomorphism, a unique finite field of order .

Galois field of order 

The unique field of order , denoted .

Structure of Finite Fields

As a group under addition,  is isomorphic to  (with *n* factors).

As a group under multiplication, the set of nonzero elements of  is isomorphic to  (and is, therefore, cyclic).

Corollary, p. 376

.

 Contains an Element of Degree *n*

Let *a* be a generator of the group of nonzero elements of  under multiplication. Then *a* is algebraic over  of degree *n*.

Subfields of a Finite Field

For each divisor *m* of *n*,  has a unique subfield of order . Moreover, these are the only subfields of .

Constructible number

A number  for which it is possible to construct a line segment of length  using a straightedge, a compass, and a line segment of length 1.

Set of constructible numbers is a field

If  and  are constructible, so are , and **.** Thus, the set of constructible numbers is a subfield of the reals and contains the rationals.

Criterion for constructability of a real number 

There is a series of fields with



such that , where , and .