

Multiplicative subgroup of a field

## Definition

Let  $k$  be a field. A multiplicative subgroup of  $k$  means a subgroup

$$U \subset k^\times$$

which is a group under multiplication.

## Theorem

Let  $U$  be a finite multiplicative subgroup of a field  $k$ . Then,  $U$  is cyclic.

## Proof

Note that  $U$  is a torsion abelian group. Let  $n$  be the smallest positive integer such that  $u^n = 1$  for all  $u \in U$ . Then,  $|U| \geq n$ . Consider the polynomial

$$f(x) = x^n - 1$$

so every  $u \in U$  is a root. Since  $f$  has at most  $n$  roots,  $|U| \leq n$ . We conclude that  $|U| = n$  and it is cyclic.

## Corollary

If  $k$  is finite, then  $k^\times$  is cyclic.

## Question

Let  $p$  be a prime. For any positive integer  $n$ , is there a finite field  $k$  of characteristic  $p$  with  $k^\times$  containing an element of order  $n$ ? If yes, what is the minimal cardinality of such a field?