

A finite subgroup of the multiplicative group of a field is cyclic

Ingredients of the proof

(1) In \mathbb{Z}_n , the number of elements of order d is precisely:

$$\begin{cases} 0 & \text{if } d \nmid n \\ |U_d| & \text{if } d|n \end{cases}$$

(2) For any n , $\sum_{d|n} |U_d| = n$.

(3) Let F be a field, U a finite subgroup of F^\times , and $n = |U|$. Then the number of elements of order d in U is:

$$\begin{cases} 0 & \text{if } d \nmid n \\ 0 \text{ or } |U_d| & \text{if } d|n \end{cases}$$

(Thus if $d|n$ there are two cases: either there is no element of order d at all, or there are exactly $|U_d|$ such elements.)

Assuming these ingredients, the theorem is proved as follows.

Proof:

Let D be the set $\{d : U \text{ has an element of order } d\}$ and let $n = |U|$. Now by (2, 3):

$$\sum_{d \in D} |U_d| = |U| = n = \sum_{d|n} |U_d|$$

Thus $\sum_{d \in D} |U_d| = \sum_{d|n} |U_d|$, and hence

$$D = \{d : d|n\}$$

In particular $n \in D$ and thus U is cyclic. ■

The three ingredients

(1) follows from our work on the group \mathbb{Z}_n , and (2) follows from (1). An example may clarify both (1) and (2): classify the elements of \mathbb{Z}_{12} according to their orders, then count the number of elements of each order and add (naturally, the total will be 12).

Point (3) is delicate. There are two points that must be checked.

(3a) If U has an element of order d then $d|n$.

(3b) If U has an element of order d then there are exactly $|U_d|$ elements of order d in U .

Now point (3a) will become clear later when we discuss Lagrange's Theorem (§7.5).

Proof of (3b):

Let $u \in U$ have order d and let $H = \{a \in U : a^d = 1\}$. Then H is a subgroup of U which contains the cyclic subgroup $\langle u \rangle$ generated by u :

$$\langle u \rangle \subseteq H; |\langle u \rangle| = d$$

In particular $|H| \geq d$. On the other hand H consists of all roots of the polynomial $x^d - 1$, of degree d ; so $|H| \leq d$. Thus $|H| = d$ and $H = \langle u \rangle$ is cyclic of order d .

This proves that H contains exactly $|U_d|$ elements of order d . ■