

Finite Multiplicative Subgroups of a Field

Let $G \subset F^*$ be a finite group. There are several ways to prove that G is cyclic. All proofs are based on the fact that the equation $x^d = 1$ can have at most d solutions in a field F .

PROOF (I) Use the structure theorem for finite abelian groups. If $|G| = n$ and G is not cyclic, then the structure theorem yields $d < n$ so that $x^d = 1$ for all $x \in G$. Contradiction. ■

PROOF (II) Give an elementary argument that if G is a finite abelian group and $x, y \in G$, then there exists $z \in G$ so that $|z| = \text{lcm}(|x|, |y|)$. Namely, if the orders of x and y are relatively prime, take $z = xy$. Otherwise, look at the prime power factorizations of the orders of x and y . Any divisor of $|x|$ will be the order of some power of x , since $\langle x \rangle$ is a cyclic group. So, you find z as a product of various powers of x and y , corresponding to the various maximal prime power factors of $|x|$ and $|y|$, as in the relatively prime case. It then follows that for a finite abelian group G there is an integer d so that G contains an element of order d and $x^d = 1$ for all x in G . Hence, if $x^d = 1$ has at most d solutions then G is cyclic. ■

PROOF (III) Suppose G is a finite group so that for each integer d the equation $x^d = 1$ has at most d solutions in G . Then, even without assuming G abelian at the outset, you can prove G is cyclic. Namely, first of all any cyclic group of order m has exactly $\phi(s)$ elements of order s , for each divisor s of m , where $\phi(s)$ is the Euler phi function. (A consequence is the Euler formula $m = \sum_{s|m} \phi(s)$, the sum taken over the divisors s of m .) Now, back to our group G . For a given divisor d of $n = |G|$, either group G has no element of order d , or it has at least one, in which case G contains a cyclic group of order d , which, by hypothesis, must contain all solutions of $x^d = 1$ in G . Thus, in this case, G contains *exactly* $\phi(d)$ elements of order d . Now, we know $|G| = n = \sum_{d|n} \phi(d)$, the sum over the divisors of n , by the Euler result. But all elements of G have some order d which divides n , and it is impossible that any order $d | n$ is “left out”, since there are either 0 or $\phi(d)$ elements of order d in G . The sum would not add up to n if 0 ever occurred. In particular, G contains elements of order n . ■