

Theorem on Classification of Cyclic Groups

Dr. Holmes

April 19, 2004

The main theorem of section 20.9 (characterization of cyclic groups) is proved using a different strategy than is used in the book. I made an error in preparing this proof and so had to “wing it” (sorry).

Further, the proof I did in class wasn't quite right either – but the one given here is easier and I think now correct. I also have a nice quick argument for Euler's formula.

Theorem: Let G be a group of order n . The following statements are equivalent.

1. G is isomorphic to C_n (G is a cyclic group).
2. There are exactly $\phi(d)$ elements of G of order d for each divisor d of n .
3. There are exactly d elements of G such that $x^d = 1$.

First we show that (1) implies (2) and (3).

Assume that G is a cyclic group of order n . Let g be an element of G of order n . Every element of G can be written in the form g^k for some k with $0 \leq k < n$, and the value of k is uniquely determined by the element of G . Suppose $x^d = 1$. Then we have $x = g^k$ for a uniquely determined k with $0 \leq k < n$, and we have $g^{kd} = 1$. This can only be true if $kd = qn$ for some q (kd must be a multiple of n), so $k = \frac{qn}{d}$. This means that k must be a multiple of $\frac{n}{d}$, and there are exactly d multiples of $\frac{n}{d}$ which are greater than or equal to 0 and less than n . Notice that if k is a multiple of $\frac{n}{d}$ then kd will be a multiple of n , so these values of k are exactly the ones which work, and there are exactly d elements x of G such that $x^d = 1$.

An element $x = g^k$ of G will have order r such that kr is the least common multiple of k and n : this implies $r = \frac{\text{lcm}(k,n)}{k} = \frac{kn}{\text{gcd}(k,n)k} = \frac{n}{\text{gcd}(k,n)}$. From this we see that $x = g^k$ has order n iff k is relatively prime to n , and so there are $\phi(n)$ elements of C_n of order n . The set of elements y of G such that $y^d = 1$ is a copy of C_d and will include all elements of G of order d : we have just shown that C_d contains $\phi(d)$ elements of order d , so G contains $\phi(d)$ elements of order d .

(2) implies (1) is easy: if a group of order n contains $\phi(d)$ elements for each element d of n , then it contains $\phi(n) \geq 1$ elements of order n : a group of order n with an element of order n is cyclic.

Now we show that (3) implies (2), which allows us to see that (1), (2), and (3) are all equivalent. This is where our proof is different from the proof in the book (and it's also where we got confused).

We do not need strong induction (I was wrong about this in class).

Let G be a group of order n such that for each divisor d of n there are exactly $\phi(d)$ elements such that $x^d = 1$.

For each divisor d of n , there is either an element of order d in the group or there is not. If there is an element of order d , the powers of this element make up a cyclic subgroup of order d (which will contain all the elements y such that $y^d = 1$) and this group will contain $\phi(d)$ elements of order d , which will be all the order d elements in the group.

All elements of G will have a divisor of n as their order, so n (the size of G) can be expressed as the sum of all the $\phi(d)$'s such that there is an element of order d in G . But $\sum_{d|n} \phi(d) = n$, so this sum must contain the $\phi(d)$'s for *all* $d|n$ in order to add up to n , and there are $\phi(d)$ elements of each order d dividing n . So (3) implies (2). Of course this immediately implies that there is an order n element, so we have (1) as well.

To see that $\sum_{d|n} \phi(d) = n$, consider the following: For any n , $\phi(n)$ is the number of positive proper fractions (fractions less than one) in simplest form with denominator n . n is the number of positive proper fractions with denominator n . But every positive proper fraction with denominator n simplifies to a uniquely determined positive proper fraction in simplest form with denominator some divisor d of n : the number of these is $\sum_{d|n} \phi(d)$, and so this must be equal to n .