MA347 – HW7

Jonathan Lam

February 15, 2021

1. Let G be a finite cyclic group of order n. Show that for each positive integer d dividing n, there exists a subgroup of order d.

   Proof. By definition, a cyclic group $\langle a \rangle$ is a group in which each element $x \in G$ can be written in the form $x = a^m$, for some $a \in G$ and $m \in \mathbb{N}$.

   We have already shown in a theorem during lecture that the order of a (finite) cyclic (sub)group $\langle a \rangle$ is the degree n of a (i.e., the smallest positive exponent of a), consisting of the (distinct) elements $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

   Now suppose $d|n$, or $\exists q \in \mathbb{N}$ such that $n = dq$. Consider the subgroup generated by $a' = a^q = a^{n/d}$, i.e., $\langle a' \rangle \leq \langle a \rangle = G$. Then d is an exponent of a', since $a'^d = a^{(n/d)d} = a^n = e$. Furthermore, for some integer d' such that $0 < d' < d$, $a'^{d'} = a^m$, where $0 < qd' = m < n$, so $a^m \in G - \{e\}$ because the elements of the cyclic group are distinct. Thus d is the degree of a. By the theorem above, $|\langle a' \rangle| = d$. □

2. Let G be a finite cyclic group of order n. Let a be a generator. Let r be an integer $\neq 0$, and relatively prime to n.

   (a) Show that a^r is also a generator of G.

   (b) Show that every generator of G can be written in this form.

   (c) Let p be a prime number, and G a cyclic group of order p. How many generators does G have?

Proof. (a) Since r, n are coprime nonzero integers, then there exists $x, y \in \mathbb{Z}$ such that $xr + (-y)n = 1 \Rightarrow xr = yn + 1$. Thus:

$$(a^r)^x = a^{rx} = a^{yn+1} = a^{yn}a = (a^n)^y a = e^y a = ea = a$$

Thus, for any $b = a^m \in G$ for some $m \in \mathbb{Z}$ such that $0 \leq m < n$, then b can be written as $(a^{rx})^m = (a^r)^{xm}$, so a^r is a generator for G.

(b) Assume that $b \in G$ cannot be written in the form a^r, where r is some nonzero integer coprime to n. Since $b \in G$, $b = a^{r'}$ for some $r' \in \mathbb{Z}$ not coprime to n, $0 \leq r' < n$.

Let $\gcd(r', n) = d > 1$. Then, $n/d, r'/d \in \mathbb{N}$, and

$$\left(a^{r'}\right)^{n/d} = a^{r'(n/d)} = a^{r'n/d} = a^{n(r'/d)} = (a^n)^{r'/d} = e^{r'/d} = e$$

Since $n, d \in \mathbb{N}$ and $d > 1$, then $n/d < n$. Thus b has a degree less than n, so the subgroup generated by b must have order less than n (by the theorem stated in the solution to (1)), so b cannot be a generator of G.

By contrapositive, if b is a generator of G, then it can be written in the form $b = a^r$, where r is a integer $\neq 0$ coprime to n.

(c) Each integer $m \in \mathbb{N}$ such that $0 < m < p$ is coprime to p. According to (a), each element of $\{a^m\}_1^{p-1} = G - \{e\}$ is a generator of G.

We can also show that e is not a generator of G (for any group with order > 1). For a finite cyclic group, the set of exponents form an ideal generated by the degree of a, i.e., the set of exponents is $J = \{xn : x \in \mathbb{Z}\}$ (theorem from lecture). Since $e = a^y$ for $y \in J$, and $d|y$, then e cannot be written in the form a^r for r, n coprime. By part (b), e is not a generator of G.

Thus G has $p - 1$ generators.

□