SUBGROUPS OF A FINITE CYCLIC GROUP

This is essentially a detailed solution to problem 3 on homework 3. I am writing it out because the result is important and the suggested proof is tricky (although very elegant).

Let G be a cyclic group of order n and let $x \in G$ be a generator. As usual, we denote by e the identity element in G. Let $H \subset G$ be a subgroup. Define $S \subset \mathbf{Z}$ by

$$S = \{i \in \mathbf{Z} \mid x^i \in H\}.$$

Proposition 1. *S is a subgroup of $\mathbf{Z}^+$.*

Proof. We have $x^0 = e$ and $e \in H$, since H is a subgroup. Since $x^0 \in H$, we get that $0 \in S$. Next, if $a, b \in S$, then $x^a, x^b \in H$. But then $x^{a+b} = x^a x^b \in H$, since H is closed under products. Therefore $a + b \in S$. Finally, if $a \in S$, then $x^a \in H$. But then $x^{-a} = (x^a)^{-1} \in H$, since H is closed under taking the inverse. Therefore $-a \in S$. Thus, S contains 0 and is closed under addition and taking negatives. Therefore, it is a subgroup of $\mathbf{Z}^+$ □

Proposition 2. *$H = \langle x^d \rangle$ for some d that divides n.*

Proof. Since $S \subset \mathbf{Z}^+$ is a subgroup, we know that $S = \mathbf{Z}d$ for some d. Furthermore, since $x^n = e$ and $e \in H$, we see that $n \in S$. Therefore, d divides n.

By the definition of S, we get

$$H = \{x^i \mid i \in S\}.$$

Since $S = \mathbf{Z}d$, we conclude that $H = \{x^{id} \mid i \in \mathbf{Z}\} = \langle x^d \rangle$. □

Proposition 3. *Let a be a positive integer. The order of x^a is $\operatorname{lcm}(a, n)/a$. In particular, if a divides n, then the order of x^a is n/a.*

Proof. Let k be the order of x^a. Then k is the smallest positive integer such that $(x^a)^k = e$. Recall that $(x^a)^i = x^{ai}$ and $x^{ai} = e$ if and only if n divides ai. Therefore, ak is the smallest positive multiple of a which is also a multiple of n. In other words, $ak = \operatorname{lcm}(a, n)$ and hence $k = \operatorname{lcm}(a, n)/a$.

If a divides n, then $\operatorname{lcm}(a, n) = n$ and hence $k = n/a$. □

Theorem 4. *Every subgroup of G is cyclic of order dividing n. Furthermore, for every positive integer a dividing n, there is a unique subgroup of G of order a.*

Proof. By Proposition 2, every subgroup of G is of the form $\langle x^d \rangle$ for some d dividing n. By Proposition 3, the order of such a group is n/d, which divides n. This proves the first sentence.

Let a be a positive integer dividing n, say $n = ab$. Then, by Proposition 3, the subgroup $\langle x^b \rangle$ of G has order a. This proves that for every positive integer a dividing n, there is a subgroup of G of order a.

Finally, let H and H' be two subgroups of G of the same order. By Proposition 2, $H = \langle x^d \rangle$ and $H' = \langle x^{d'} \rangle$ for some d and d' dividing n. By Proposition 3, the order of H is n/d and the order of H' is n/d'. Since the orders are equal, we conclude that $d = d'$ and hence $H = H'$. This proves that G has a unique subgroup of a given order. □

Example 5. Let us take $G = \langle x \rangle$ to be of order 12. Then all the subgroups of G are as follows:

- Order 1: $\langle x^{12} \rangle = \{x^0\}$
- Order 2: $\langle x^6 \rangle = \{x^0, x^6\}$
- Order 3: $\langle x^4 \rangle = \{x^0, x^4, x^8\}$
- Order 4: $\langle x^3 \rangle = \{x^0, x^3, x^6, x^9\}$
- Order 6: $\langle x^2 \rangle = \{x^0, x^2, x^4, x^6, x^8, x^{10}\}$
- Order 12: $\langle x \rangle = \{x^0, x^1, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}\}$