MARCH 12 NOTES

1. Section 5: Subgroups

Before the exam, we defined the notion of **subgroup**.

Definition 1.1. A **subgroup** H of a group G is a subset $H \subset G$ such that:

1. (1) H is nonempty, which we usually check as: $e \in H$ (where $e \in G$ is the identity of G),
2. (2) H is closed under the binary operation $\star$ in G, and
3. (3) H is closed under inverses.

Today, we will classify subgroups of cyclic groups.
First, remember that we showed:

Proposition 1.2. *For any group G and any $x \in G$, $\langle x \rangle$ is a subgroup of G.*

In fact, if G is cyclic, these are *all* of the possible subgroups.

Theorem 1.3. *Let G be a cyclic group and x a generator of G, so $G = \langle x \rangle$. If H is any subgroup of G, then $H = \langle x^m \rangle$ for some $m \geq 0$. In particular, every subgroup of G is cyclic.*

Proof. Let $H \subset G$. If $H = \{e\}$, then $H = \langle e \rangle = \langle x^0 \rangle$. Now, suppose $H \neq \{e\}$, so H contains some element $x^k \in G$ for $k \neq 0$. Because H is closed under inverses, we may assume that $k > 0$ (if H contained x^{-k}, it must also contain x^{+k}). Let m be the smallest positive power of x that appears in H. We will show that $H = \langle x^m \rangle$.

First, because H is a subgroup and $x^m \in H$, any power of x^m must also be in H. This follows because H is closed under multiplication and inverses. Therefore, $\langle x^m \rangle \subset H$. Now, suppose $x^n \in H$ for some $n \in \mathbb{Z}$. By the division algorithm, we may write $n = mq + r$ for some $0 \leq r < m$. Because $x^n \in H$ and $x^m \in H$, we know $(x^m)^{-q} = x^{-mq} \in H$, so $x^n x^{-mq} \in H$ because H is closed under multiplication. But, $x^n x^{-mq} = x^{n-mq} = x^r \in H$, and $0 \leq r < m$. Because m was the smallest positive power of x that appeared in H and $r < 0$, this is only possible if $r = 0$. Therefore, $n = mq$ and hence $x^n = (x^m)^q \in \langle x^m \rangle$. Therefore, $H \subset \langle x^m \rangle$. This proves that $H = \langle x^m \rangle$. □

Example 1.4. List all subgroups of $\mathbb{Z}_4$.

By the previous theorem, since $\mathbb{Z}_4 = \langle 1 \rangle$, every subgroup is of the form $\langle m \rangle$ for some $m \in \mathbb{Z}_4$. Listing these, we find all of the subgroups:

$$\langle 0 \rangle = \{0\}, \quad \langle 1 \rangle = \{0, 1, 2, 3\} = \langle 3 \rangle, \quad \langle 2 \rangle = \{0, 2\}.$$

In the previous example, we see that 1 and 3 generate the same subgroup. We can make this precise for any n:

Theorem 1.5. *If $G = \langle x \rangle$ is cyclic with $|G| = n$, then the distinct subgroups are*

$$\{\langle x^d \rangle \mid d \text{ is a divisor of } n\}.$$

If d is a divisor of n, $\langle x^d \rangle = \langle x^k \rangle$ is and only if $\gcd(k, n) = d$.

Proof. Let H be a subgroup of G. If $H = \langle e \rangle$, then $H = \langle x^n \rangle$ and n is a divisor of n, so the statement holds. Now, assume $H \neq \langle e \rangle$. By the proof of the previous theorem, $H = \langle x^d \rangle$ where d is the smallest positive power of x in H. We want to show that d divides n. By the division algorithm, we can write $n = qd + r$ for some $0 \leq r < d$. Because $x^n = e$, we know $x^n \in H$, and because $x^d \in H$, $x^{qd} \in H$. Therefore, $x^n x^{-qd} = x^r \in H$, but $r < d$ and d was the smallest positive power of x appearing in H. Therefore, $r = 0$, so $n = qd$ which implies that d divides n.

This shows that every subgroup $H \subset G$ is of the form $\langle x^d \rangle$ where d is a divisor of n.

By the results on order, if $H = \langle x^k \rangle$ for any $k \in \mathbb{Z}$, $|H| = o(x^k) = \frac{n}{\gcd(k,n)}$. If d is a divisor of n, this proves that $|H| = \frac{n}{d}$, which implies that any two distinct divisors of n correspond to distinct subgroups of G (because they have different sizes).

Now, let d be a divisor of n. Assume $d = \gcd(k,n)$, so d divides k, i.e. $k = md$ for some integer m. Then, $x^k = x^{md} = (x^d)^m$, so $x^k \in \langle x^d \rangle$ and hence $\langle x^k \rangle \subset \langle x^d \rangle$. But, by the formula for order, $\langle x^k \rangle$ has $\frac{n}{d}$ elements, and so does $\langle x^d \rangle$, so we must have $\langle x^k \rangle = \langle x^d \rangle$.

Similarly, suppose $\langle x^k \rangle = \langle x^d \rangle$. Then, these sets must have the same size, so $\frac{n}{\gcd(k,n}) = \frac{n}{\gcd(d,n)} = \frac{n}{d}$, so $\gcd(k,n) = d$. Therefore, we have shown $\gcd(k,n) = d$ if and only if $\langle x^k \rangle = \langle x^d \rangle$. □

Revisiting the previous example, we can now list all subgroups of $\mathbb{Z}_n$ for any n. The theorem tells us that they are just all possible subgroups $\langle d \rangle$ for d some divisor of n.

Example 1.6. What are the subgroups of $\mathbb{Z}_4$? Because the divisors of 4 are $1, 2, 4$, the subgroups are:

$$\langle 1 \rangle = \{0,1,2,3\}; \quad \langle 2 \rangle = \{0,2\}; \quad \langle 4 \rangle = \langle 0 \rangle = \{0\}.$$

Example 1.7. What are the subgroups of $\mathbb{Z}_{12}$? The divisors of 12 are $1, 2, 3, 4, 6, 12$, so we have one subgroup for each divisor:

$$\langle 1 \rangle = \mathbb{Z}_{12}, \quad \langle 2 \rangle = \{0,2,4,6,8,10\}, \quad \langle 3 \rangle = \{0,3,6,9\},$$
$$\langle 4 \rangle = \{0,4,8\}, \quad \langle 6 \rangle = \{0,6\}, \quad \langle 12 \rangle = \{0\}.$$