Friday, Sept. 14

Last time, we ended with...

Cor: The subgroups of \( \mathbb{Z} \) are exactly the subgroups \( n\mathbb{Z}, \, n \in \mathbb{Z} \).

But if \( n < 0 \), then \( n \mathbb{Z} = (-n)\mathbb{Z} \) with \( -n > 0 \), so we may assume \( n > 0 \).

Moreover, these are all different, since for any \( H \leq \mathbb{Z} \),

\[
\begin{align*}
\text{\( n = \{ \)} & \text{the smallest element of } H \cap \mathbb{Z}^+ \text{ (if } H \cap \mathbb{Z}^+ \neq \emptyset) \\
\text{or} & \text{ } 0 \\
\text{(and } n \in N). & \text{ (otherwise)}
\end{align*}
\]

Divisors and Greatest Common Divisors

Def: Let \( a, b \in \mathbb{Z} \). We say that \( a \) divides \( b \), and write \( a \mid b \), if \( aq = b \) for some \( q \in \mathbb{Z} \). (If \( a \mid b \), we also say \( b \) is a multiple of \( a \).)

If \( a \neq 0 \): \( \frac{b}{a} \in \mathbb{Z} \).

Otherwise: \( 0 \mid b \iff b = 0 \).

Def: Let \( r \) and \( s \) be integers (possibly \( 0 \)).

The subset \( H = \{nr + ms : \, n, m \in \mathbb{Z} \} \) is a subgroup of \( \mathbb{Z} \), so \( H = d\mathbb{Z} \) for some (uniquely defined) \( d \in \mathbb{N} \).

We say that \( d \) is the greatest common divisor (gcd) of \( r \) and \( s \), and write \( d = \gcd(r, s) \).

Both \( r = 1 \cdot r + 0 \cdot s \) and \( s = 0 \cdot r + 1 \cdot s \) lie in \( H \), so \( d \mid r \) and \( d \mid s \). Therefore \( d \) is a common divisor of \( r \) and \( s \).
Useful Fact: Since $d \in H$, we can write $d = nr + ms$ for some $n, m \in \mathbb{Z}$.

\[ \text{if } e \text{ is a common divisor of } r \text{ and } s, \]
\[ \text{then } e | nr \text{ and } e | ms, \text{ so } e | d. \]
\[ \therefore e \leq d \quad (\text{unless } d = 0) \]

Examples:
\[ \gcd(24, 10) = 2 \]
\[ \gcd(0, 14) = 14 \]
\[ \gcd(0, -14) = 14 \]
\[ \gcd(0, 0) = 0 \]

Subgroups of Finite Cyclic Groups

Thm: Let $G$ be a finite cyclic group of order $n$, and let $a \in G$ be a cyclic generator. (So $G = \langle a \rangle$)

Let $b \in G$, write $b = a^s$ for some $s \in \mathbb{Z}$, and let $d = \gcd(s, n)$.

Then $\langle b \rangle = \langle a^d \rangle$, and this cyclic subgroup has order $n/d$.

Also $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(s, n) = \gcd(t, n)$.

Proof: Since $d = \gcd(s, n)$, we have $d = un + vs$ (with $u, v \in \mathbb{Z}$).

Then $a^d = (a^n)^u \cdot (a^s)^v = a^u \cdot b^v = b^v$, so $a^d \in \langle b \rangle$.

\[ \langle a^s \rangle \leq \langle b \rangle \]

Also $d | s$, say $d \cdot w = s$, so $b = a^s = (a^d)^w \in \langle a^d \rangle$.

\[ \langle b \rangle \leq \langle a^d \rangle. \]

\[ \therefore \langle b \rangle = \langle a^d \rangle. \]

The elements of $G$ are $e, a, a^2, \ldots, a^{n-1}$ (all different).

The elements of $\langle a^d \rangle$ are $e, a^d, a^{2d}, \ldots, (a^d)^{\frac{n}{d}-1}$ (all different).

$a^d$ has order $\frac{n}{d}$ (since $(a^d)^{\frac{n}{d}} = a^n = e$ but no smaller power $> 0$ is $e$).
\[ |<b>| = |<a^d>| = |a^d| = n/d. \]

For the last sentence:
\[ <a^2> = <a^k> \Rightarrow |a^k| = (a^k) \Rightarrow \frac{n}{gcd(s,n)} = \frac{n}{gcd(t,n)} \Rightarrow gcd(s,n) = gcd(t,n) \]
\[ gcd(s,n) = gcd(t,n) \Rightarrow <a^2> = <a^{gcd(s,n)}> = <a^{gcd(t,n)}> = <a^k>. \]

Cor. (not in book): Let \( G \) be a finite cyclic group of order \( n \), and let \( m \in \mathbb{Z}^+ \). Then \( G \) has a subgroup of order \( m \) if and only if \( m | n \).

If so, it has exactly one such subgroup equal to \( <a^{n/m}> \) for any cyclic generator \( a \) of \( G \).

Proof: Let \( a \) be a cyclic generator, and let \( H \leq G \).

Then \( H \) is cyclic, so \( H = <a^s> \) for some \( s \in \mathbb{Z} \), and by the previous theorem, \( |H| = \frac{n}{gcd(s,n)} \), which divides \( n \).

\[ \therefore G \text{ has a subgroup of order } m \Rightarrow m | n. \]

Conversely, if \( m | n \) then \( G \) has exactly one subgroup \( <a^{n/m}> \) of order \( m \), because \( \frac{n}{gcd(n,m)} = \frac{n}{n/m} = m \), so \( G \) has a subgroup of order \( m \).

Next (3rd) sentence: Suppose \( m | n \) and \( H_1 \leq G \), \( H_2 \leq G \) with \( |H_1| = |H_2| = m \). Then \( H_1 = <a^s> \) and \( H_2 = <a^t> \) for some \( s, t \in \mathbb{Z} \), and \( \frac{n}{gcd(s,1)} = |H_1| = m = |H_2| = \frac{n}{gcd(n,t)} \)

\[ \therefore gcd(s,1) = gcd(n,t) \Rightarrow H_1 = <a^s> = <a^t> = H_2. \]

\[ \therefore G \text{ has exactly one such subgroup, and it equals } <a^{n/m}> \text{ by this}. \]