2.3 Cyclic Groups

Def: A group is cyclic if it is generated by one element, i.e. \( G = \{ x^n \mid n \in \mathbb{Z} \} \) for some \( x \in G \).
We write \( G = \langle x \rangle \) to indicate \( G \) is generated by \( x \).

Prop: The map \( \mathbb{Z} \to G = \langle x \rangle \) defined by
\[ m \mapsto x^m \]
is a homomorphism.

Proof: This simply means \( x^{m_1+m_2} = x^{m_1} x^{m_2} \)
for all \( m_1, m_2 \in \mathbb{Z} \). See Exercise 19, §1.1.

Then the kernel \( \{ m \in \mathbb{Z} \mid x^m = 1 \} \) is a subgroup of \( \mathbb{Z} \).

Prop: All subgroups \( G \subset \mathbb{Z} \) are of the form \( n\mathbb{Z} \)
for a unique integer \( n \geq 0 \).

Proof: Either \( G = \{ 0 \} \) or \( G \) contains a nonzero element \( m \). If \( m < 0 \), its inverse \( -m \) is \( > 0 \).

Thus \( G \) contains a positive element.
By the Well Ordering Property of \( \mathbb{Z} \), there is a least positive element \( n \) of \( G \).

We claim \( G = n\mathbb{Z} \). Suppose \( m \in G \).

By the Division Algorithm, there are unique integers \( q, r \) such that \( m = qn + r \) and \( 0 \leq r < n \). Since \( m \in G \) and \( n \in G \), and \( G \) is a group, we have \( r = m - qn \in G \).

If \( r > 0 \), that contradicts the assumption that \( n \) is the least positive element of \( G \). Hence, \( r = 0 \) and \( m = qn \), proving \( G = n\mathbb{Z} \).

---

\( n\mathbb{Z} \) acts on \( \mathbb{Z} \) by addition. The cosets form the additive group \( \mathbb{Z}/n\mathbb{Z} \).

Prop: If \( G = \langle x \rangle \) is cyclic of order \( n \), the map \( m \mapsto x^m \) gives an isomorphism
of \( \mathbb{Z}/n\mathbb{Z} \) onto \( G \). (Shorthand notation: \( \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \))

If \( G \) is cyclic of infinite order, then \( m \mapsto x^m \) gives an isomorphism of \( \mathbb{Z} \) onto \( G \).

**Prop:** If \( G = \langle x \rangle = \mathbb{Z}_n \) then the element \( x^a \) has order \( \frac{n}{(a,n)} \).

Thus, the subgroup generated by \( x^a \) has order \( \frac{n}{(a,n)} \).

The subgroups of \( G = \langle x \rangle = \mathbb{Z}_n \) are in one-to-one correspondence with the divisors \( d \mid n \), the correspondence being \( d \mapsto \langle x^\frac{n}{d} \rangle \).

**Proof:** \((x^a)^k = x^{ak} = 1\) if and only if \( n \mid ak \).

Let \( d = (a,n) \), \( a = a'd \), \( n = n'd \). Then \((a',n') = 1\).

So \((x^a)^k = 1\) iff \( n' \mid a'k \) by cancelling \( d \),

iff \( n' \mid k \) since \((a',n') = 1\).

The smallest such \( k \) is \( k = n' = \frac{n}{(a,n)} \). \( \blacksquare \)
2.3 - 4

Suppose $H$ is a subgroup of $G \cong \mathbb{Z}_n$.

Consider the homomorphism $\varphi : \mathbb{Z} \to G$

defined by $\varphi(m) = x^m$.

Prop: For any homomorphism $\varphi : G \to H$ and

any subgroup $J \subseteq H$, the inverse image $\varphi^{-1}(J) = \{g \in G | \varphi(g) \in J\}$ is a subgroup.

So for our $\varphi : \mathbb{Z} \to G$, $\varphi^{-1}(H)$ is a

subgroup $d\mathbb{Z}$ of $\mathbb{Z}$.

The kernel is $\varphi^{-1}(1) = n\mathbb{Z}$.

We know $\varphi^{-1}(1) \subseteq \varphi^{-1}(H)$. Hence, $n\mathbb{Z} \subseteq d\mathbb{Z}$.

This means $d / n$ and that $H$ is generated

by $x^d$. So $H$ has order $\frac{n}{(d,n)} = \frac{n}{d}$.

Replacing $d$ by $\frac{n}{d}$ (also a divisor of $n$), we can say

$H$ is $\langle x^{\frac{n}{d}} \rangle$ of order $\frac{n}{n/d} = d$. \[\]
#21-23 Binomial Theorem

\[(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k\]

where \(\binom{n}{k} = \frac{n!}{k! (n-k)!} = \frac{n(n-1) \cdots (n-k+1)}{k!}\)

(Proved by induction)

If \(n = p\) is prime, then \(p \mid \binom{p}{k}\) for \(1 \leq k \leq p-1\),

That's because \(p \nmid p!\) but \(p \nmid k! (p-k)!\) for \(1 \leq k \leq p-1\).

#21: Show \((1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}\)

but \((1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}\) for \(n \geq 2\)

(This proves \(1+p\) has order \(p^{n-1}\))

Use proof by induction, and

\[(1+p)^{p^n} = ((1+p)^{p^{n-1}})^p\]
ALTERNATIVE: Just prove 
\[(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}} \text{ for } n \geq 1.\]

The first case is \(n = 2\):
\[(1+p)^2 \equiv 1 \pmod{p^2},\]
and \(1+p \not\equiv 1 \pmod{p^2}.\)

The second statement is clearly true since \(p^2 \not| p\).

\[(1+p)^p = \sum_{k=0}^{p} \binom{p}{k} p^k,\]

For \(k > 1\), either \(p \nmid \binom{p}{k}\) and \(p \nmid p^k\)
or \(k = p\) and then \(p^2 \nmid p^p\).

In all cases, all these terms are \(\equiv 0 \pmod{p^2}\).

Thus, \((1+p)^p \equiv 1 \pmod{p^2}, \checkmark.\)

Induction step:

Assume \((1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}\) for all \(2 \leq m \leq N\) and \((1+p)^{p^{m-2}} \not\equiv 1 \pmod{p^m}\).

Write \((1+p)^{p^{m-2}} = 1 + \alpha p^{n-1}\) for some integer \(\alpha\).

We know \(\alpha \neq 0 \pmod{p}\) because ?

Now prove \((1+p)^{p^{m+1}} \equiv 1 + \alpha p^n \pmod{p^{n+1}}\). Etc.