§2.2 A nonempty subset of Group $G$

$C_G(A) = \{ g \in G \mid g a g^{-1} = a \ \forall a \in A \}$

$Z(G) = C_G(G)$

$N_G(A) = \{ g \in G \mid g A g^{-1} = A \}$

Group actions: Kernel, $G$ acts on $S \subseteq S$

$G_s = \{ g \in G \mid g \cdot s = s \}$

Example

$(PC(G)$ set of subsets of $G$)

Then $G$ acts on $PC(G)$ by conjugations

for $x \in G$

$g \cdot x = g x g^{-1}$

(Take $g \cdot \emptyset = g \emptyset g^{-1} = \emptyset$)

Note that this is a group action

Kernel of the action is the center of $G$, $Z(G)$

for nonempty $X \subseteq G$

$G_X = N_G(X)$

stabilizer of $X$ under this action

Note, since $g \emptyset g^{-1} = \emptyset$, $G \emptyset = G = : N_G(\emptyset)$

The Centralizer of a set $A$, $C_G(A) = \{ g \in G \mid \forall a \in A, g a g^{-1} = a \}$ i.e. $g$ that commute with $A$

The Center of $G$, $Z(G) = C_G(G) = \{ g \in G \mid \forall a \in G, g a g^{-1} = a \}$

The normalizer of $A$ is $N_G(A) = \{ g \in G \mid g A g^{-1} = A \}$

If $G$ is a group acting on set $S$

The stabilizer is $G_S$

The Kernel is $Ker(G)$

$G$ acts on itself $G$ (left regular) conjugation $f g.s \rightarrow g.sg^{-1}$
$N_G(A)$ acts on $A$

special case is $G$ on itself

$N_G(A)$ acts on $A$ via conjugation:
for $g \in N_G(A)$, $g \cdot a = gag^{-1}$
so the Kernel is $C_G(A)$

1. In particular, in (1) if we take $A = G$, then $N_G(A) = G$ and we get the "more famous" action of $G$ on itself by conjugation.

Note that the Kernel of this action is $Z(G)$.

Why not $g^{-1}a = g$ ? Not a left action in this case.

§ 2.3 Cyclic Groups

Def: A (multiplicative) group $G$ is cyclic if $\exists g \in G$ s.t. $G$ is generated by $g$, that is $G = \{g^n \mid n \in \mathbb{Z}\}$

(An additive group $A$ is cyclic if $A = \{na \mid n \in \mathbb{Z}\}$)

Examples

$\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z}/m\mathbb{Z} = \langle 1 \rangle = \{[n] \mid n \in \mathbb{Z}\}$

Notice $N_G(A)$ acts on $A$ by conjugation $g \cdot a = gag^{-1}$, so the Kernel of this action is $C_G(A)$, i.e. set of $gag^{-1} = a$, elements which commute with elements of $A$.

If $G$ acts on itself by conjugation, then its Kernel is $Z(G)$.

Cyclic groups are given by the powers of a generating element.
Ex. 3 \( G = \{ 1, e, \frac{2\pi i}{n}, \frac{2(2\pi i)}{n}, \ldots, \frac{(n-1)(2\pi i)}{n} \} \)

Then \( (G, \cdot) \) is cyclic.

Prop. Let \( G = \langle g \rangle \) be a multiplicative cyclic group.

Then there is a surjective homomorphism

\[ \mathbb{Z} \to G \]

\[ m \mapsto g^m \]

and is injective iff \( G \) is infinite.

\( \text{Pf.} \) The exponential rule shows \( f \) is a group homomorphism.

Surjectivity is immediate, as is the injectivity of \( f \).

N.T.S. infinite \( \Rightarrow \) injective.

If \( G \) infinite but \( f \) not injective, then \( \exists m, i > j \) such that \( g^i = g^j \) so

\[ g^{i-j} = g^0 = 1 \]

hence \( f(i-j) = f^0 = 1 \).

It follows that \( G = \{ 1, g^1, g^2, \ldots, g^{m-1} \} \) using the Division Algorithm.

Lemma \( G = \langle g \rangle \) a cyclic group.

Then \( \lvert G \rvert = \lvert g \rvert \)

\( \text{Proof.} \) Suppose \( m = \lvert g \rvert < \infty \) then as above

\[ G = \{ 1, g, g^2, \ldots, g^{m-1} \} \]

Moreover \( \{ g, \ldots, g^{m-1} \} \) distinct.

\( \mathbb{Z} \) is homomorphic to any cyclic group, and is injective iff \( G \) is an infinite group.

\( \lvert \langle g \rangle \rvert = \lvert g \rvert \)

i.e. orders are preserved.
Suppose not defined
\[ \exists \ g^i = g^j \]
\[ \text{But then } g^i \cdot g^{-i} = 1 \quad \text{with} \quad 0 < i-j < m \quad \iff \quad |g| = m \]
\[ \therefore \ |g| = \infty, \text{ lemma follows} \]
\[ \text{when } |g| = \infty, \ |G| = \infty \ \square \]

**LEMMA**
Let group \( g \in G \) has order \( m < \infty \).
Then \( g^n = 1 \) for \( n \in \mathbb{Z} \) if \( m \mid n \).

**Proof**
By Division Algorithm
\[ n = q m + r \quad \text{with} \quad 0 \leq r < m \]
So,
\[ g^n = (g^m)^q \cdot g^r = g^r \]
Since \( 0 < r < m \),
\[ g^n = g^r = 1 \]
\[ \therefore \ r = 0 \ \iff \ m \mid n \ \square \]

**Prop**
Let \( G = \langle g \rangle \) cyclic.
\[ |G| = |g| = m < \infty \]
Then isomorphism \( \phi : \mathbb{Z}/m\mathbb{Z} \rightarrow G \)
\[ \phi : \mathbb{Z}/m\mathbb{Z} \rightarrow G \]
\[ \overline{n} \rightarrow g^n \]
If \( p^2 \mid m \) then \( \phi \) is well-defined. Suppose \( n \sim n' \) (mod \( m \)),
\[ n' = n + km \]
\[ g^{n'} = g^{n+km} = g^ng^km = g^n(g^m)^k = g^n \]
\( Z/m\mathbb{Z} \) isomorphic to \( G \), cyclic group of order \( m \)
\[ |g| = m \quad \text{then} \quad g^n = 1 \iff \ m \mid n \]
To show \( \varphi \) injective

\[ \varphi(l) = \varphi(l') \Rightarrow g^l = g^{l'} = g^{l-l'} = 1 \]

from before \( m | l-l' \Rightarrow l \equiv l' \text{ in } \mathbb{Z}/m\mathbb{Z} \)

\[ a \overline{1} = \overline{l} \]

Thus \( \varphi \) injective

Since \( |\mathbb{Z}/m\mathbb{Z}| = |G| \) surjective + injective \( \Rightarrow \) bijective

To see \( \varphi \) a homomorphism

\[ \varphi(i+j) = \varphi(i) \varphi(j) = g^i g^j = \varphi(i) \varphi(j) \]

For positive \( m \), take \( \mathbb{Z}_m \) to be the multiplicative cyclic group of order \( m \)

Remind: \( \mathbb{Z}/m\mathbb{Z} \) is the additive group

**Theorem**: \( G = \langle g \rangle \) cyclic

i) Every subgroup of \( G \) is cyclic

ii) If \( |g^i| = \infty \) then \( \langle g^i \rangle = \langle g^d \rangle \text{ iff } i \equiv d \mod m \)

iii) Suppose \( |g^i| = m < \infty \) then

\[ |g^{i+k}l| = \frac{m}{(l,m)} \text{ (as } GCD) \]

Moreover \( \langle g^i \rangle = \langle g^{i+k}l \rangle \)

If \( G \) a cyclic group

- the subgroups are cyclic

- if \( |g^i| = \infty \) then \( \langle g^i \rangle = \langle g^d \rangle \text{ iff } i \equiv d \mod m \)

- \( |g^i| = m, \text{ then } |g^{i+k}l| = \frac{m}{(l,m)} \)
PROOF

(i) \( H \leq G \) wlog \( H \neq \langle 1 \rangle \)

Now let \( m \) be least positive integer s.t. \( g^m \in H \)

Choose arbitrary \( g \in H \)

Then \( e = g^m + r \) for some \( 0 \leq r < m \) by Division

\[ g^r = g^{e - gm} = (g^e)(g^{-m})^r \in H \quad \therefore r = 0 \text{ by choice of } m \]

\[ g^r = g^m = (g^m)^r \]

Thus \( H \leq \langle g^m \rangle \)

and since \( g^m \in H \), \( \langle g^m \rangle \subseteq H \) so \( H = \langle g^m \rangle \)

And so \( H \) is cyclic.

(ii)

Note \( g^a = g^b \Rightarrow g^{a-b} = 1 \Rightarrow a = b \) since \( |g| = 100 \)

Next \( i, j \in \mathbb{Z} \)

\( \langle g^i \rangle = \langle g^j \rangle \) if and only if \( \langle g^i \rangle \subseteq \langle g^j \rangle \) and vice versa

\[ \iff g^i = (g^j)^r \quad \text{and} \quad g^j = (g^i)^s \quad \forall \ r, s \in \mathbb{Z} \]

\[ \iff i = jr \quad \text{and} \quad j = is \]

\[ \iff j = \pm i \]
(iii) Set \( n = 1g^f \)

Then \( (g^f)^{m/(l,m)} = (g^m)^{l/(l,m)} = 1 \)

Therefore \( n | m/(l,m) \)

on the other hand

\( g^{ln} = 1 \)

\( \therefore m | ln \), also by earlier

\( \therefore \frac{m}{(l,m)} \bigg| \frac{ln}{(l,m)} n \)

Since \( \frac{m}{(l,m)} \) and \( \frac{ln}{(l,m)} \) relatively prime, it follows that \( \frac{m}{(l,m)} | n \)

Therefore \( n = \frac{m}{(l,m)} \) by Fundamental Theorem of Arithmetic

For the rest, by Euclid's algorithm \( \exists u, v \in \mathbb{Z} \)

set \( ul + vm = (l, m) \)

And so \( g^{(l,m)} = g^u g^v = g^u \in <g^f> \)

Thus \( <g^{(l,m)}> \subseteq <g^f> \)

But \( g^f \in <g^{(l,m)}> \) because \( (l, m) \bigg| l \)

Therefore \( <g^f> = <g^{(l,m)}> \)

Concluding §2.3 New Homework, Due Tues
§ 2.4 GENERATING A SUBGROUP

**Lemma.** Let \( H_\alpha \) be a subgroup of \( G \) for all \( \alpha \in A \)

Then \( K = \bigcap_{\alpha \in A} H_\alpha \) is a subgroup of \( G \).

First, \( K \) is non-null since \( 1 \in H_\alpha \).

Next,

\[
x, y \in \bigcap_{\alpha \in A} H_\alpha \\
x y^{-1} \in H_\alpha \text{ for all } \alpha \in A \\
\Rightarrow x y^{-1} \in \bigcap_{\alpha \in A} H_\alpha = K
\]

**Definition.** \( A \subseteq G \) then take the subgroup generated by \( A \)

\( \langle A \rangle = \bigcap_{\alpha \in \mathbb{H} \subseteq \mathbb{G}} H_\alpha \) that is, smallest subgroup containing \( A \).

**Notation.** When \( A = \{ a_1, \ldots, a_m \} \), we write \( \langle a_1, \ldots, a_m \rangle \equiv \langle A \rangle \).

And when \( A = \{ a \} \), write \( \langle a \rangle \equiv \langle A \rangle \).

Notice if \( K = \bigcap_{\alpha \in A} H_\alpha \), then \( K \) is also a subgroup \( K \subseteq H_\alpha \subseteq G \).

\( \langle A \rangle \) is the smallest subgroup containing \( A \), i.e. \( \bigcap_{\alpha \in \mathbb{H} \subseteq \mathbb{G}} H_\alpha \).