Definition. A group homomorphism \( \phi : G \to G' \) is an isomorphism if \( \phi \) is a bijection. If there is an isomorphism between \( G \) and \( G' \) we say \( G \) and \( G' \) are isomorphic. This is denoted by \( G \cong G' \).

Given a homomorphism \( \phi : G \to G' \) there are subgroups of each that can indicate to us whether \( \phi \) is injective or surjective.

Definition. Let \( \phi : G \to G' \) be a homomorphism. Define \( \ker(\phi) = \{ g \in G : \phi(g) = e_{G'} \} \). This is called the kernel of \( \phi \). Define \( \text{im}(\phi) = \{ \phi(g) : g \in G \} \). This is called the image of \( \phi \). We usually use the notation \( \phi(G) \) for \( \text{im}(G) \).

Example. If \( \phi : GL_2(\mathbb{R}) \to \mathbb{R}\setminus\{0\} \) is given by \( \phi(A) = \det(A) \) then \( \ker(\phi(A)) = SL_2(\mathbb{R}) \) and \( \text{im}(\phi) = \mathbb{R}\setminus\{0\} \).

Theorem 1 Let \( \phi : G \to G' \) be a homomorphism. Then

1. \( \ker(\phi) \) is a subgroup of \( G \), and \( \phi \) is injective if and only if \( \ker(\phi) = e_G \).
2. \( \text{im}(\phi) \) is a subgroup of \( G' \), and \( \phi \) is surjective if and only if \( \text{im}(\phi) = G' \) (or equivalently, \( \phi(G) = G' \)).

Proof. 1. If \( a, b \in \ker(\phi) \), then \( \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e_{G'}(e_{G'})^{-1} = e_{G'} \) so by the Subgroup Test, \( \ker(\phi) \) is a subgroup.

Now if \( \ker(\phi) = \{ e \} \) then
\[
\phi(a) = \phi(b) \implies \phi(ab^{-1}) = e \implies ab^{-1} = e \implies a = b.
\]

Moreover, if \( \phi \) is injective, then
\[
\phi(a) = e \implies \phi(a) = \phi(e) \implies a = e,
\]

so \( \ker(\phi) = \{ e \} \).

2. Exercise.

Example. Following the examples we have from last class. We see:

1. If \( \phi : GL_n(\mathbb{R}) \to \mathbb{R}\setminus\{0\} \) is given by \( \phi(A) = \det(A) \) then \( SL_2(\mathbb{R}) = \ker(\phi) \) so \( \phi \) is not injective. \( \phi \) is surjective: indeed for any non-zero real number \( k \), the diagonal matrix with \( k \) in the top left corner and 1s elsewhere has determinant \( k \).
2. If $V$ and $W$ are vector spaces and $T : V \rightarrow W$ is a linear transformation, define $\phi : V \rightarrow W$ by $\phi(v) = T(v)$. Then whether or not $\phi$ is injective and/or surjective depends on $V, W$ and $T$.

3. If $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ is given by $\phi(a) = a \mod n$, then $\ker(\phi) = n\mathbb{Z}$, so $\phi$ is not injective. However, $\phi$ is surjective.

4. Let $\phi : \mathbb{R} \rightarrow \mathbb{R}_{>0}$ be given by $\phi(a) = e^a$. Then $\ker(\phi) = \{0\}$ since $e^a = 1$ implies $a = 0$. Hence, $\phi$ is injective. Now for any $a \in \mathbb{R}_{>0}$, $\phi(\log(a)) = e^{\log(a)} = a$, so $\phi$ is surjective.

5. If $I : G \rightarrow G$ is given by $I(g) = g$, then $I$ is certainly surjective and $\ker(\phi) = \{e\}$, so $I$ is an isomorphism.

6. Let $\phi : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ be given by $\phi(\sigma) = 1$ if $\sigma$ is an odd permutation and $1$ if $\sigma$ is an odd permutation. Then $\ker(\phi) = A_n$, the set of even permutations, so $\phi$ is not injective. However, since $\phi((12)) = 1$ and $\phi(e) = 0$, $\phi$ is surjective.

**Proposition 2** The homomorphism $\phi : G \rightarrow G'$ is an isomorphism if and only if there exists a homomorphism $\psi : G' \rightarrow G$ such that $\phi \circ \psi = \psi \circ \phi$ are identity maps on their respective groups.

**Proof Sketch** Define $\psi(a)$ to be the unique pre-image of $a$ under $\phi$. Since $\phi$ is a bijection, this is well defined and $\phi \circ \psi = \psi \circ \phi$ are identity maps between their respective groups. One needs to check $\psi$ is indeed a homomorphism, but this effectively comes for free since $\phi$ is one.

1 **Cyclic Groups**

Now that we've introduced the concept of isomorphism, we can study general groups, up to isomorphism. The first class of groups of interest are the ones with simplest possible structure, those generated by a single element.

**Definition.** A group $G$ is cyclic if $G$ can be generated by a single element, i.e. there is some $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$.

Remember, $g^n$ here means applying the group product to $g$. So, if $G$ is a group under $+$ for example, then $G = \{ng \mid n \in \mathbb{Z}\}$.

**Example.**

1. $\mathbb{Z}$ is an infinite cyclic group generated by $1$.

2. $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group generated by $[1]$.

3. The subset $\{1, r, r^2, \ldots, r^{n-1}\}$ in $D_{2n}$ is a subgroup that is cyclic. It is generated by $r$.

Note: If $H$ is a cyclic group there may be many candidates for a generator of $H$. For example, $\mathbb{Z}$ is also generated by $-1$. 

2
Theorem 3 Suppose $G$ is cyclic and $G = \langle g \rangle$. Then $|G| = |g|$. This is a consequence of the following observations:

1. If $|g| = \infty$, then $g^a \neq g^b$ for any $a \neq b$ in $\mathbb{Z}$, so $|G| = \infty$

2. If $|g| = n < \infty$, then $g^n = 1$ and $\{1, g, g^2, \ldots, g^{n-1}\}$ is the set of distinct elements of $G$, so $|G| = n$.

Proof. 1) Suppose $G$ is infinite and for contradiction suppose there were integers $a < b$ such that $g^a = g^b$. Then $g^{b-a} = 1$, which implies $g$ has finite order, a contradiction. Thus the elements in the set $\{g^n \mid n \in \mathbb{Z}\}$ are all distinct, so $G$ is infinite.

2) Consider when $|g| = n$. Then by definition $g^n = 1$. The elements $\{1, g, g^2, \ldots, g^{n-1}\}$ are all distinct because, if otherwise, then there are distinct integers $0 \leq a < b < n$ such that $g^a = g^b$, which then implies $g^{b-a} = 1$, which contradicts $|g| = n$ because $0 \leq b-a < n$. We now claim that for any $t \in \mathbb{Z}$, $t \notin \{0, 1, 2, \ldots, n-1\}$, that $g^t \in \{1, g, g^2, \ldots, g^{n-1}\}$. Indeed, by the Division Algorithm we can write $t =qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Then

\[ g^t = g^{qn+r} = (g^n)^q \cdot g^r = g^r. \]

We conclude $G \subseteq \{1, g, g^2, \ldots, g^{n-1}\}$. Since $G \supseteq \{1, g, g^2, \ldots, g^{n-1}\}$, we conclude $G = \{1, g, g^2, \ldots, g^{n-1}\}$.

What is the structure of cyclic groups and their subgroups? That is the content of the next theorem:

Theorem 4 Let $G$ be a cyclic group. Every subgroup of $G$ is cyclic.

Proof. Let $H \leq G$. If $H = \{1\}$, the trivial subgroup, then we are done. Otherwise, let $n$ be the smallest positive power of $g$ that lies in $H$. That is, $g^n \in H$ but $g^k \notin H$ for any positive integer $k < n$. We claim $H = \langle g^n \rangle$. Suppose otherwise for contradiction. Then there exists an integer $t$ that is not a multiple of $n$ such that $g^t \in H$. By the Division Algorithm, there exist integers $q, r$ with $0 \leq r < n$ such that $t = qn + r$. This implies

\[ g^r = g^{t-qn} = g^t(g^n)^{-q} \in H, \]

contradicting that $n$ is the smallest positive integer for which $g^n \in H$. Thus $t$ is a multiple of $n$ and hence $H \subseteq \langle g^n \rangle$. Since $\langle g^n \rangle \subseteq H$ we conclude $H = \langle g^n \rangle$, so $H$ is cyclic.