Math 371 Lecture #34
§7.8 (Ed.2), 8.4 (Ed.2): Quotient Groups and Homomorphisms, Part II

We develop some of the basic theory of homomorphisms, culminating in the First and Third Isomorphism Theorems. (Yes, there is a Second Isomorphism Theorem which you have as a homework problem.)

Lemma 8.19. Let \( f : G \to H \) be a homomorphism of groups with kernel \( K \). For \( a, b \in G \) we have \( f(a) = f(b) \) if and only if \( Ka = Kb \).

Proof. Suppose that \( f(a) = f(b) \). Then \( f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = e_H \), so that \( ab^{-1} \in K \), so that \( Ka = Kb \).

Now suppose that \( Ka = Kb \).
Then \( ab^{-1} \in K \) and so \( f(ab^{-1}) = e_H \).

Hence
\[
f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e_H.
\]

This implies that \( f(a) = f(b) \).

First Isomorphism Theorem. If \( f : G \to H \) is a surjective homomorphism of groups with kernel \( K \), then \( G/K \) is isomorphic to \( H \).

Proof. We define a map \( \varphi : G/K \to H \) by \( \varphi(Ka) = f(a) \).

First we show that this map is well-defined.

For \( Ka = Kb \), we know that \( f(a) = f(b) \) by Lemma 8.19 (Ed.3), so that \( \varphi(Ka) = \varphi(Kb) \), meaning that \( \varphi \) is well-defined.

Second we show that \( \varphi \) is surjective.

For any \( h \in H \), there exists \( a \in G \) such that \( f(a) = h \) by the surjectivity of \( f \).

Then \( \varphi(Ka) = f(a) = h \), so that \( \varphi \) is surjective.

Third we show that \( \varphi \) is injective.

Suppose that \( \varphi(Ka) = \varphi(Kb) \).

Then \( f(a) = f(b) \) which implies by Lemma 8.19 (Ed.3) that \( Ka = Kb \), so that \( \varphi \) is injective.

Last we show that \( \varphi \) is a homomorphism.

For \( Ka, Kb \in G/K \) we have
\[
\varphi((Ka)(Kb)) = \varphi(K(ab)) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb).
\]

Therefore, \( \varphi \) is an isomorphism.

Example. What is \( \mathbb{Z} \times \mathbb{Z}/\langle (2, 2) \rangle \) isomorphic to? Is it \( \mathbb{Z} \)? or \( \mathbb{Z}_2 \)? or something else?
The element \( \mathbb{Z} \times \mathbb{Z} + (1, 0) \) has infinite order while the element \( \mathbb{Z} \times \mathbb{Z} + (1, 1) \) has order 2. We consider the map \( f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_2 \) defined by

\[
f(a, b) = (a - b, [b]_2).
\]

We show that \( f \) is surjective.

For \((c, [d]_2) \in \mathbb{Z} \times \mathbb{Z}_2\), the choice of \(a = c\) and \(b = 0\) if \(d\) is even, or \(a = c + 1\) and \(b = 1\) if \(d\) is odd, satisfies \(f(a, b) = (c, [d]_2)\).

We show that \( f \) is a homomorphism.

For \((a, b)\) and \((c, d)\) in \(\mathbb{Z} \times \mathbb{Z}\) we have

\[
f((a, b) + (c, d)) = f(a + c, b + d) = (a + c, [b + d]_2) = (a, [b]_2) + (c, [d]_2) = f(a, b) + f(c, d).
\]

We show that the kernel of \( f \) is \(\langle (2, 2) \rangle\).

For \((a, b) \in \mathbb{Z} \times \mathbb{Z}\), the equation \(f(a, b) = (0, 0)\) implies that \(a - b = 0\) and \([b]_2 = 0\). Thus \(a = b\) and \(b\) is even, say \(b = 2k\) for some \(k \in \mathbb{Z}\), so that \((a, b) = (2k, 2k)\).

Since every element of \(\langle (2, 2) \rangle\) has the form \((2k, 2k)\) for some \(k \in \mathbb{Z}\), we have that the kernel of \( f \) is \(\langle (2, 2) \rangle\).

By the First Isomorphism Theorem, we have \(\mathbb{Z} \times \mathbb{Z} / \langle (2, 2) \rangle \cong \mathbb{Z} \times \mathbb{Z}_2\).

Now we consider subgroups of a quotient group \(G/N\) and how these subgroups are related to \(G\) and \(N\).

**Theorem 8.21.** If \(N\) is a normal subgroup of a group \(G\) and \(K\) is any subgroup of \(G\) that contains \(N\) (i.e., \(N \subseteq K \subseteq G\)), then \(K/N\) is a subgroup of \(G/N\).

**Proof.** With \(N\) a subgroup of \(K\) and \(K\) a subgroup of \(G\), the normality of \(N\) in \(K\) follows because \(Na = aN\) for all \(a \in G\) implies \(Na = aN\) for all \(a \in K\).

Then \(K/N\) is a group whose elements are the cosets \(Na\) for \(a \in K\).

Since \(K\) is a subgroup of \(G\), each element of \(K/N\) is a element of \(G/N\). 

**Third Isomorphism Theorem.** If \(K\) and \(N\) are normal subgroups of a group \(G\) with \(N \subseteq K \subseteq G\), then \(K/N\) is a normal subgroup of \(G/N\) and \((G/N)/(K/N) \cong G/K\).

**Proof.** If we can construct a surjective homomorphism from \(G/N\) to \(G/K\) with kernel \(K/N\), then the First Isomorphism Theorem will imply that \((G/N)/(K/N) \cong G/K\).

Define a map \(f : G/N \to G/K\) by \(f(Na) = Ka\).

The map \(f\) is well-defined, because for \(Na = Nb\) we know that \(ab^{-1} \in N\), and since \(N \subseteq K\), then \(ab^{-1} \in K\), so that \(Ka = Kb\).

The surjectivity of \(f\) follows because any \(Ka\) in \(G/K\) is the image of \(Na \in G/N\).

The map \(f\) is a homomorphism because for \(Na, Nb \in G/N\) we have

\[
f((Na)(Nb)) = f(N(ab)) = K(ab) = (Ka)(Kb) = f(Na)f(Nb).
\]
To identify the kernel of $f$ we suppose that $f(\text{Na}) = \text{Ke}$, which says that $Ka = Ke$.

However $Ka = Ke$ if and only if $a = ae^{-1} \in K$, and so the kernel of $f$ is precisely those cosets Na with $a \in K$, namely $K/N$.

By the First Isomorphism Theorem we obtain $(G/N)/(K/N) \cong G/K$. \hfill \Box

Example. A normal subgroup of $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is $N = \{1, 4\}$.

A normal subgroup of $U_{15}$ that contains $N$ is $K = \{1, 2, 4, 8\}$.

A normal subgroup of $U_{15}/N = \{N, N2, N7, N11\}$ is $K/N = \{N, N2\}$.

By the Third Isomorphism Theorem, $(U_{15}/N)/(K/N) \cong U_{15}/K = \{K, K11\}$.

Corollary 8.23. Let $N$ be a normal subgroup of a group $G$ and let $K$ be any subgroup of $G$ that contains $N$. Then $K$ is normal in $G$ if and only if $K/N$ is normal in $G/N$.

Proof. Suppose $K$ is normal in $G$. Then by the Third Isomorphism Theorem, the subgroup $K/N$ is normal in $G/N$.

Now suppose that $K/N$ is a normal subgroup of $G/N$. We will show that for any $a \in G$ and any $k \in K$ we have $a^{-1}ka \in K$, implying that $K$ is normal in $G$.

Since $K/N$ is normal, we have

$$N(a^{-1}ka) = (Na^{-1})(Nk)(Na) = (Na)^{-1}(Nk)(Na) \in K/N.$$ 

This means that $N(a^{-1}ka) = Nt$ for some $t \in K$, and hence $a^{-1}ka = nt$ for some $n \in N$. Since $N \subseteq K$, we have $n \in K$ so that $nt \in K$, meaning that $a^{-1}ka \in K$. \hfill \Box

Theorem 8.24. Let $N$ be a normal subgroup of a group $G$. If $T$ is a subgroup of $G/N$, then there exists a subgroup $H$ of $G$ that contains $N$ such that $T = H/N$.

Proof. We use the subgroup $T$ of $G/N$ to construct a subgroup $H$ of $G$: set

$$H = \{a \in G : Na \in T\}.$$ 

This is a subgroup of $H$: for $a, b \in H$, we have $N(ab^{-1}) = Na[Nb^{-1}] \in T$ because $T$ is subgroup.

We show next that $N \subseteq H$: for $a \in N$, we have $ae^{-1} = ae = a \in N$, so that $Na = Ne$, and since $Ne \in T$, we obtain $a \in H$.

Now we recognize that $H/N$ consists of the cosets $Na$ for $a \in H$, which implies that $H/N = T$. \hfill \Box

Definition. A group $G$ is called simple if its only normal subgroups are $\{e\}$ and $G$, i.e., it has no proper normal subgroup.

Theorem 8.25. An abelian group $G$ is simple if and only if it is isomorphic to $\mathbb{Z}_p$ for some positive prime $p$.

Proof. If $G$ is isomorphic to $\mathbb{Z}_p$ then it simple because the only subgroups (normal or otherwise) of $\mathbb{Z}_p$ are $\{e\}$ and $\mathbb{Z}_p$. 

Now suppose that $G$ is simple.
Since $G$ is abelian, every subgroup of $G$ is normal, and with $G$ simple, there are no proper subgroup of $G$.
Hence for a non-identity element $a \in G$, the cyclic subgroup $\langle a \rangle = G$.
Then $G$ is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some integer $n \geq 2$.
Since $\mathbb{Z}$ has many proper subgroups like $\langle 2 \rangle$, we have that $G$ is not isomorphic to $\mathbb{Z}$.
Thus $G$ is isomorphic to $\mathbb{Z}_n$ for some $n \geq 2$.
If $n$ is not prime then $\mathbb{Z}_n$ has proper normal subgroups, and so $G$ must be isomorphic to $\mathbb{Z}_p$ for some prime $p \geq 2$. 
\hfill \square