Mike O'Sullivan
Department of Mathematics
San Diego State University

Math 627A: Modern Algebra I

Notes on the Isomorphism Theorems for Groups

1 Fundamental Results: Up to the First Isomorphism Theorem

The material up to the first isomorphism theorem deals with basic properties of

1. Groups

2. Homomorphisms of groups

3. Injective homomorphisms (subgroups)

4. Surjective homomorphisms (quotient groups)

A brief comment about items (3) and (4). If H is a subgroup of G the inclusion map is an injective homomorphism from H to G. On the other hand, the image of an injective homomorphism $\alpha : H \longrightarrow G$ is a subgroup that is isomorphic to H. So the study of injective homomorphisms is (up to isomorphism) the study of subgroups.

After studying subgroups, we defined normal subgroup and showed several equivalent properties determining that a subgroup is normal. If N is normal in G, we can define a quotient group G/N. The first isomorphism theorem shows that any surjective homomorphism is (up to isomorphism) a quotient group of the domain.

Theorem 1.1 (First Isomorphism). *Let $\phi : G \longrightarrow H$ be a surjective homomorphism with kernel N. Then G/N is isomorphic to H.*

Here are a two short, "just use the definitions," exercises.

Exercise 1.1. Let $\phi : G \longrightarrow H$ be a homomorphism of groups. If A is a subgroup of G and B is a subgroup of H then $\phi(A)$ is a subgroup of H and $\phi^{-1}(B)$ is a subgroup of G.

Exercise 1.2. Let $\alpha : G \longrightarrow H$ and $\beta : H \longrightarrow K$ be homomorphisms of groups. Then $\beta \circ \alpha$ is a homomorphism from G to K.

Here is a typical snappy use of the 1st isomorphism theorem.

Theorem 1.2. *Let* $G_1, G_2, \ldots G_r$ *be groups and let* $N_1, N_2, \ldots, N_r$ *be normal subgroups,* $N_i \trianglelefteq G_i$. *Then*

$$(G_1 \times G_2 \times \cdots \times G_r)/(N_1 \times N_2 \times \cdots \times N_r) \cong (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r)$$

Proof. Check that the function

$$G_1 \times G_2 \times \cdots \times G_r \longrightarrow (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r),$$

which is just projection onto each factor, is a homomorphism. The kernel is $(N_1 \times N_2 \times \cdots \times N_r)$. The 1st isomorphism theorem now gives the result. $\qquad\square$

2 Structure in the Quotient Group: The Third Isomorphism Theorem and the Correspondence Theorem

The next step is to understand the structure of a quotient group. The two main results—the third isomorphism theorem and the correspondence theorem—have fairly simple statements, which obscure some subtle issues. The proof of the third isomorphism theorem is an easy consequence of the first isomorphism theorem.

Theorem 2.1 (Third Isomorphism). *Let* N *and* K *be normal subgroups of* G *with* N *contained in* K . *Then* $G/K \cong (G/N)\big/(K/N)$.

Proof. We have two well defined quotient groups: G/N and G/K . I claim there is a well defined function from G/N to G/K taking gN to gK . To prove this we have to check that if two cosets aN and bN are equal then the cosets aK and bK are also equal. This follows from $aN = bN$ iff $a^{-1}b \in N$. Since and $N \leq K$, $aN = bN$ implies $a^{-1}b \in K$ so $aK = bK$.

It is easy to check that the function defined above is surjective and a homomorphism. So the result follows from the first isomorphism theorem. $\qquad\square$

The correspondence theorem gives a more precise analysis of a quotient group. In G/N , we have to be careful how we write elements, subgroups and cosets of subgroups.

Suppose N is normal in G and H is a subgroup of G containing N .

$$H/N = \{hN : h \in H\}$$
$$G/N = \{gN : g \in G\}$$

It is easy to show that H/N is a subgroup of G/N.

We write cosets of H/N as

$$aN(H/N) = aN\{hN : h \in H\}$$
$$= \{ahN : h \in H\}$$

When are two cosets equal?

$$
\begin{aligned}
aN(H/N) = bN(H/N) &\iff bN \in aN(H/N) \\
&\iff bN = ahN \text{ for some } h \in H \\
&\iff b = ahn \text{ for some } h \in H \text{ and } n \in N \\
&\iff b = ah' \text{ for some } h' \in H \text{ (here } h' = hn) \\
&\iff aH = bH
\end{aligned}
$$

This shows that we have a well defined map from cosets of H to cosets of H/N (taking aH to $aN(H/N)$) and that it is injective. It is clearly surjective, so the number of cosets of H in G equals the number of cosets of H/N in G/N.

Let's look at the condition for the normality of H/N:

$$aN(H/N)(aN)^{-1} = \{aha^{-1}N : h \in H\}$$

This is equal to H/N iff $aHa^{-1} = H$. So H/N is normal in G/N iff H is normal in G.

Let $\pi : G \to G/N$ be the canonical map. From an exercise in the previous section, we know that $\pi(H)$ is a subgroup of G/N for any subgroup of G. If we restrict to *subgroups containing N* then π is injective on subgroups: $\pi(H) = \pi(K)$ implies $H = K$. To prove this, suppose H and K contain N. Let $h \in H$ and $hN \in K/N$. Then $hN = kN$ for some $k \in K$, so $h = kn$ for some $n \in N$. Since $N \subseteq K$ we have $h = kn \in K$. Thus if H is not contained in K then H/N is not contained in K/N. In particular, if $H \neq K$ then $\pi(H) \neq \pi(K)$.

On the other hand, and subgroup Q of G/N is the image of some subgroup of G, namely, $\pi(\pi^{-1}(Q))$. Thus we have the 1-1 correspondence of the theorem.

Theorem 2.2 (Correspondence). *Let N be a normal subgroup of G and let $\pi : G \to G/N$ be the canonical homomorphism. There is a one-to-one correspondence between subgroups of G/N and subgroups G containing N, given by π. The correspondence respects containment and normality. That is for H, K containing N:*

- $K \leq H$ *iff* $K/N \leq H/N$, *and in this case* $[H : K] = [H/N : K/N]$.

- K *is normal in G iff K/N is normal in G/N.*

3 Interaction between Two Subgroups: The Second Isomorphism Theorem

We now consider two subgroups of a group G and prove several results about the interaction between them. At first we make no additional assumptions on the two groups, then we assume that one is normal, and finally that both are.

Lemma 3.1. *Let K, H be subgroups of G. The following are equivalent:*

1. *$G = KH$ and $K \cap H = \{e_G\}$*

2. *Every element of G can be uniquely written as kh for $k \in K$ and $h \in H$.*

Proof. $G = KH$ says that every element of G can be written in the form kh.
$K \cap H = \{e_G\}$ gives uniqueness $k_1 h_1 = k_2 h_2$ implies $k_1^{-1} k_2 = h_1 h_2^{-1}$ and this must be the identity. Thus $h_1 = h_2$ and $k_1 = k_2$. $\qquad\square$

Lemma 3.2 ([A] 1.3.6). *Let H, K be subgroups of G.*

$$HK = KH \quad \Longleftrightarrow \quad HK \text{ is a subgroup of } G$$

Proof. $\Longrightarrow$ HK is closed under inversion: $(hk)^{-1} = k^{-1} h^{-1} \in KH = HK$.
HK is closed under multiplication: $HKHK = HHKK = HK$.

$\Longleftarrow$ Since HK is closed under inversion, $HK = (HK)^{-1} = K^{-1} H^{-1} = KH$. $\qquad\square$

Suppose now that H, N are subgroups of G with N *normal in* G.

- $HN = NH$ since $gN = Ng$ for any $g \in G$.

- HN is a subgroup of G by the lemma.

- N is normal in HN, since it is normal in any subgroup of G that contains it.

Theorem 3.3 (Second Isomorphism). *Let N be normal in G and H a subgroup of G. Then $H \cap N$ is normal in H and $H/(H \cap N) \cong HN/N$.*

Proof. Consider $G \xrightarrow{\pi} G/N$ restricted to the subgroup H. The kernel is $H \cap N$. The image is $HN/N = \{hN : h \in H\}$. By the 1st isomorphism theorem, $H/(H \cap N) \cong HN/N$. $\quad\square$

The following special case is of interest.

Corollary 3.4. *Let $H \leq G$ and $N \trianglelefteq G$. If $G = HN$ and $H \cap N = \{e_G\}$ then $G/N \cong H$. In other words, there is an exact sequence*

$$0 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 0$$

Definition 3.5. In the situation of the corollary we say that G is the *semi-direct product* of N by H and we write $G \cong N \ltimes H$.

Corollary 3.6. *Suppose $K \not\trianglelefteq G$ and $N \not\trianglelefteq G$ and $G = KN$ and $K \cap N = \{e_G\}$. Then elements of K and N commute: for any $k \in K$ and $n \in N$, $kn = nk$. Furthermore, $G \cong K \times N$.*

Proof. It is sufficient to show that $knk^{-1}n^{-1} = e$. Since N is normal $knk^{-1} \in N$ and therfore $knk^{-1}n^{-1} \in N$. Similar reasoning shows $knk^{-1}n^{-1} \in K$. Now $K \cap N = \{e\}$ gives the result.

Consider the map $K \times N \xrightarrow{\phi} G$ defined by $(k, n) \longmapsto kn$. The map is well defined. It is injective since $kn = e$ gives $k = n^{-1} \in K \cap N = \{e\}$. It is surjective since $G = KN$. It respects multiplication:

$$\phi((k_1, n_1)(k_2, n_2)) = \phi((k_1 k_2, n_1 n_2)) = k_1 k_2 n_1 n_2 = k_1 n_1 k_2 n_2 = \phi((k_1, n_1))\phi((k_2, n_2))$$

$\square$

Definition 3.7. In the situation of the last corollary, G is often called the *internal direct product* of K and N.

The distinction between internal direct product and the usual (external) direct product of two arbitrary groups G and H is not very important. Let $\overline{G} = G \times \{e_H\}$ and similarly for $\overline{H}$. Then $G \times H$ is the internal direct product of $\overline{G}$ and $\overline{H}$.

4   Finitely Generated Abelian Groups

We will write the group operation additively. For A an abelian group, $a \in A$, and m an integer, $mA = a + \cdots + a$ with m summands. The order of a is the smallest positive integer m such that $ma = 0$. One can check that $ma + na = (m + n)a$ and $(mn)a = m(na)$.

Definition 4.1. Let p be a prime. A p-group is one in which all elements have order a power of p. For A an abelian group we define the p-group of A to be $A(p) = \{a \in A : \operatorname{ord}(a) = p^k \text{ for some } k\}$.

The fact that $A(p)$ is a group follows from the basic result that if a and b commute, then the order of $a + b$ divides $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$.

Lemma 4.2. *Let A be an abelian group of order $n = p^k m$ with p prime and m not divisble by p. Let $A(p)$ be the p-group of A and let $B = \{a \in A : ma = 0\}$. Then $A \cong A(p) \times B$.*

Proof. First of all we note that B is a group. The proof is similar to the observation we made for $A(p)$. For $b, b' \in B$, the order of $b + b'$ divides $\operatorname{lcm}(\operatorname{ord}(b), \operatorname{ord}(b'))$. This last expression is a factor of m since both $\operatorname{ord}(b)$ and $\operatorname{ord}(b')$ divide m. Thus $b + b' \in B$.

We will show that $A(p) \cap B = \{0\}$ and $A(p) + B = A$ and conclude, by Corollary 3.6, that $A \cong A(p) \times B$. An element of $A(p) \cap B$ has order that is a power of p and also divides m. Since p and m are coprime this element can only be the identity. Let a be an arbitrary element of A, and let its order be $p^s t$ with $t \mid m$. We have $p^s a \in B$ and $ta \in A(p)$ since $p^s a$ order t and ta has order p^s. Since $p \nmid t$ there are integers x, y such that $1 = xp^s + yt$. Then $a = (xp^s a + yta) = x(p^s a) + y(ta)$ can be expressed as a sum of an elment in $A(p)$ and one i B. $\square$

Theorem 4.3. *Let A be a finite abelian group. The A is isomorphic to the direct product of its p-groups. That is, if $|A| = p_1^{e_1} \ldots p_r^{e_r}$ then $A \cong A(p_1) \times \cdots \times A(p_r)$.*

Proof. For the purposes of this proof, lets define the index of A to be the number of distinct primes for which there exists an element of A with that order. Notice that if $\operatorname{ord}(a) = qm$ then $\operatorname{ord}(ma) = q$. So if the index is 1, then every element of A has order a power of some prime p. Thus the base case is immediate: if the index is 1, then $A = A(p)$ for some prime p.

Assume that the statement of the theorem is true for all primes with index less than r, let A have index r, and let p be a prime for which $A(p)$ is nonempty. By the lemma $A \cong A(p) \times B$ where B is the subgroup of elements of A with order not divisible by p. The index of B is less than r, so the induction applies. Clearly, for any $q \neq p$, $B(q) = A(q)$. This gives the result. $\square$

The previous theorem is the first step in the classification of finite abelian groups. The next step is to classify p-groups. The key lemma follows. Its proof is quite technical and not very illuminating, so we state it without proof.

Lemma 4.4. *Let A be a p-group and let a be an element of maximal order. Then $A = \langle a \rangle + K$ for some subgroup K of A*

Theorem 4.5. *Let A be a p-group. Then A is the direct product of cyclic groups each of order a power of p. Consequently, the order of A is also a power of p.*

The decomposition is unique (up to reordering). Put another way, two p-groups are isomorphic iff their decompositions have the same number of factors for each power of p.

Proof. The proof is by induction. Using the lemma we can write $A = \langle a \rangle + K$. The subgroup $\langle a \rangle$ is cyclic of order p^k for some k. Applying the induction hypothesis to K gives the result. Since A is the direct product of groups of order a power of p, A itself must have order a power of p.

Clearly, if two groups have the same number of factors for each power of p they are isomorphic. To prove the converse, consider the groups $p^i A$ and the quotients $p^i A / p^{i-1} A$. It can be shown that each of the quotients is a vector space over $\mathbb{F}_p$ (which is just $\mathbb{Z}_p$ considered as a field). The list of dimensions $\dim_{\mathbb{F}_p} p^{i-1} A / p^i A$ can be used to recover the number of $\mathbb{Z}_{p^i}$-factors for each i. $\square$

From the two previous theorems we obtain the fundamental theorem.

Theorem 4.6 (Fundamental Theorem of Finite Abelian Groups). *Let A be an abelian group of order $p_1^{e_1} \ldots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

$$A(p_i) \cong Z_{p_i^{a_{i,1}}} \times Z_{p_i^{a_{i,2}}} \times \ldots Z_{p_i^{a_{i,s_i}}}$$

then for each i, $\sum_{\ell=1}^{s_i} a_{i,\ell} = e_i$. The decomposition is unique, up to reordering.

Definition 4.7. The groups $\mathbb{Z}_{p^a}$ occurring in the decomposition are called the *elementary divisors* of A.