Lecture Notes for Math 627A
Modern Algebra
Notes on the Isomorphism Theorems for Groups

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
www-rohan.sdsu.edu/ ~ mosulliv

October 17, 2012

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)

Let's discuss (3). Suppose H is a subgroup of G. There is a function from H to G, which is called the *inclusion map*, that simply takes $h \in H$ to itself, as an element of G. Since H is a subgroup of G (it's multiplication is the same as the one on G), the inclusion map is an injective homomorphism from H to G.

On the other hand, suppose that H and G are arbitrary groups and that $\varphi : H \longrightarrow G$ is an injective homomorpism. The first exercise below shows, in particular, that $\varphi(H)$ is a subgroup of G. Thus $\varphi : H \longrightarrow \varphi(H)$ is a bijective homomorphism. This shows that the image of an injective homomorphism $\varphi : H \longrightarrow G$ is a subgroup that is isomorphic to H. Thus, the study of injective homomorphisms is essentially 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 for any surjective homomorphism $\varphi : G \longrightarrow H$, the codomain is essentially a quotient of G.

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

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

Exercises 1.2. Let $\varphi : G \longrightarrow H$ be a homomorphism of groups. If A is a subgroup of G and B is a subgroup of H then $\varphi(A)$ is a subgroup of H and $\varphi^{-1}(B)$ is a subgroup of G.

Exercises 1.3. 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 1.4. *Let $G_1, G_2, \dots G_r$ be groups and let $N_1, N_2, \dots, N_r$ be normal subgroups, $N_i \trianglelefteq G_i$. There is a well defined map*

$$\begin{aligned}(G_1 \times G_2 \times \cdots \times G_r)/(N_1 \times N_2 \times \cdots \times N_r) &\longrightarrow (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r)\\ (g_1, g_2, \dots, g_r)\, N_1 \times N_2 \times \cdots \times N_r &\longmapsto (g_1N_1, g_2N_2, \dots g_rN_r)\end{aligned}$$

and it is an isomorphism.

Proof. First we note that the function

$$G_1 \times G_2 \times \cdots \times G_r \xrightarrow{\varphi} (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r),$$

which is just projection onto each factor, is a homomorphism. This is an easy computation; let $(g_1, g_2, \dots, g_r)$ and $(g_1', g_2', \dots, g_r')$ be elements of $G_1 \times G_2 \times \cdots \times G_r$. Then

$$\begin{aligned}\varphi((g_1, g_2, \dots, g_r) * (g_1', g_2', \dots, g_r')) &= \varphi(\,(g_1g_1', g_2, g_2', \dots, g_rg_r')\,)\\ &= (g_1g_1'N_1, g_2g_2'N, \dots, g_rg_r'N_r)\\ &= (g_1N_1, g_2N, \dots, g_rN_r) * (g_1'N_1, g_2'N, \dots, g_r'N_r)\end{aligned}$$

We used, in order, the definition of multiplication in $G_1 \times G_2 \times \cdots \times G_r$, the definition of φ, the definition of multiplication in $G_1/N_1 \times G_2/N/2 \times \cdots \times G_r/N_r$.

The kernel of φ is the set of $(g_1, \dots, g_r)$ such that $g_1N_1, g_2N_2, \dots, g_rN_r = N_1 \times N_2 \times \cdots \times N_r$. Each g_i must be in N_i. So, the kernel is $N_1 \times N_2 \times \cdots \times N_r$. The 1st isomorphism theorem now gives the result. □

A generalization of the first isomorphism theorem that we will often use treats the case when φ is not necessarily injective.

Theorem 1.5 (Factor)**.** *Let $\varphi : G \longrightarrow H$ be a homomorphism with kernel N. Then φ can be factored into the canonical surjective homomorphism $\pi : G \longrightarrow G/N$ followed by an injective homomorphism $\bar{\varphi} : G/N \longrightarrow H$.*

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 $N \leq K$. Then $G/K \cong (G/N)\Big/(K/N)$.*

Proof. We have two well defined quotient groups: G/N and G/K. I claim that 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. Suppose $aN = bN$. Then $a^{-1}b \in N$ and since $N \subseteq K$ we have $a^{-1}b \in K$. Consequently $aK = bK$.

It is easy to check that the function $\varphi : G/N \longrightarrow G/K$ defined above is surjective and a homomorphism. Given any gK there is an element, namely gN, that clearly maps to it, $\varphi(gN) = gK$, so we get surjectivity. Finally, φ respects multiplication: $\varphi(gN * g'N) = \varphi(gg'N) = gg'K = gK * g'K = \varphi(gN) * \varphi(g'N)$

The kernel of φ is $\{gN : gK = eK\} = K/N$. Now the result follows from the first isomorphism theorem. □

Theorem 2.2 (Correspondence)**.** *Let $\varphi : G \longrightarrow H$ be a surjective homomorphim with kernel N. There is a one-to-one correspondence, given by φ, between subgroups of G/N and subgroups G containing N.*

$$\begin{aligned} G &\longrightarrow H \\ N \leq A &\longleftrightarrow \varphi(A) \\ \varphi^{-1}(B) &\longleftrightarrow B \end{aligned}$$

The correspondence respects containment, normality, and quotients.

- *$N \leq A \leq A'$ iff $\varphi(A) \leq \varphi(A')$.*
- *A is normal in G iff $\varphi(A)$ is normal in H. In this case $G/A \cong H/\varphi(A)$*

Proof. Some of these results are simply based on facts about functions. Let $f : X \to Y$ and let $A \subseteq X$ and $B \subseteq Y$. Then $A \subseteq f^{-1}(f(A))$ and $f(f^{-1}(B)) \subseteq B$. On the other hand, if f is surjective then for each $b \in B$ there is some $x \in X$ such that $f(x) = b$. Thus for f surjective, $f(f^{-1}(B)) = B$. Respecting containment is also immediate: If $A \subseteq A' \subseteq X$ then $f(A) \subseteq f(A')$ and similarly if $B \subseteq B' \subseteq Y$ then $f^{-1}(B) \subseteq f^{-1}(B')$.

Let A be a subgroup of G containing N and let B be a subgroup of H. We already know that $\varphi(A)$ is a subgroup of H and $\varphi^{-1}(B)$ is a subgroup of G. Based on the above discussion, to show the one-to-one correspondence, we need to show that $\varphi^{-1}(\varphi(A)) \subseteq A$. Let $g \in \varphi^{-1}(\varphi(A))$. Then $\varphi(g) = \varphi(a)$ for some $a \in A$. Consequently, $\varphi(ga^{-1}) = e_H$ and therefore $ga^{-1} \in \ker(\varphi) = N$. Since $N \subseteq A$, $ga^{-1} \in A$ so $g \in A$. Thus $\varphi^{-1}(\varphi(A)) = A$. Thus, we have established the one-to-one correspondence.

We have also shown that if B is normal then $\varphi^{-1}(B)$ is normal. These results are true for an arbitrary homomorphism. Let's now show that when φ is surjective, if A is normal in G then $\varphi(A)$ is normal in H.

Let $h \in H$. We need to show $h\varphi(A)h^{-1} = \varphi(A)$, or equivalently, $h\varphi(a)h^{-1} \in \varphi(A)$ for all $a \in A$. Since φ is surjective, there is some $g \in G$ such that $\varphi(g) = h$.

$$h\varphi(a)h^{-1} = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(gag^{-1}) \in \varphi(A)$$

The last step holds because A is normal in G, so $gag^{-1} \in A$.

Now we apply the first isomorphism theorem. Let B be normal in H. We have a composition of surjective homomorphisms

$$G \longrightarrow H \longrightarrow H/B$$

whose kernel is $\varphi^{-1}(B)$. Letting $A = \varphi^{-1}(B)$, the first isomorphism theorem says that $G/A \cong H/\varphi(A)$. □

We can derive the 3rd isomorphism theorem as a corollary.

Corollary 2.3 (3rd isomorphism theorem)**.** *Let N and K be normal subgroups of G with $N \leq K$. Then $G/K \cong (G/N)\Big/(K/N)$.*

Proof. Apply the correspondence theorem to $G \longrightarrow G/N$. The subgroup K of G corresponds to the subgroup K/N of G/N. Thus $G/K \cong (G/N)\Big/(K/N)$. □

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. $G = KH$ is equivalent to saying that every element of G can be written in the form kh.

We'll next show $K \cap H = \{e_G\}$ iff any expression for $g \in G$ as kh is unique. Suppose $K \cap H = \{e_G\}$ and $k_1h_1 = k_2h_2$. Then $k_1^{-1}k_2 = h_1h_2^{-1}$. Since this is in

both K and in H, it must be the identity. Therefore, $h_1 = h_2$ and $k_1 = k_2$, which proves uniqueness.

Now suppose that, $K \cap H \neq e_G$; say $g \in K \cap H$ is not equal to e_G. Setting $h = g$ and $k = e_G$ or $h = e_G$ and $h = g$ gives two different ways to express g in the form kh. Thus we have non-uniqueness. □

As a prelude to the second isomorphism theorem we have the following lemma.

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

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

Proof. Suppose $HK = KH$. Then HK is closed under inversion: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.
HK is also closed under multiplication: $HKHK = HHKK = HK$. This shows HK is a subgroup of G.

Suppose HK is a subgroup of G. Since HK is closed under inversion, $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. □

Suppose now that H, N are subgroups of G with N *normal in* G. We can conclude the following.

- $HN = NH$ since $gN = Ng$ for any $g \in G$.
- HN is therefore 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, call the homomorphism $\pi' : H \longrightarrow G/N$. The kernel is $H \cap N$. The image is $HN/N = \{hN : h \in H\}$. By the 1st isomorphism theorem, $H/(H \cap N) \cong HN/N$. □

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 *internal semi-direct product* of N by H and we write $G \cong N \ltimes H$.

Note the order is important: $N \ltimes H$ and $H \ltimes N$ mean two different things. The first assumes N is normal in G and the second assumes H is normal in G. If both H and N are normal then the two semidirect products are isomorphic to each other and to the direct product, as the following corollary shows.

Corollary 3.6. *Suppose $K \trianglelefteq G$ and $N \trianglelefteq G$ 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 therefore $knk^{-1}n^{-1} \in N$. Similarly, since K is normal, $nk^{-1}n^{-1} \in K$ so $knk^{-1}n^{-1} \in K$. Now $K \cap N = \{e\}$ gives the result.

Consider the map $K \times N \xrightarrow{\varphi} G$ 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 (so is a homomorphism):

$$\begin{aligned} \varphi((k_1, n_1)(k_2, n_2)) &= \varphi((k_1k_2, n_1n_2)) \\ &= k_1k_2n_1n_2 = k_1n_1k_2n_2 \\ &= \varphi((k_1, n_1))\varphi((k_2, n_2)) \end{aligned}$$

Thus φ is an isomorphism. □

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 subtle, and not, to my mind very important. In $G \times H$, 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 $\overline{H}$.

One can also define the external semi-direct product of of two groups. Sorry, no time to write about that now.

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 $A(p) = \{a \in A : \text{ord}(a) = p^k \text{ for some } k\}$.

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 $\text{lcm}(\text{ord}(a), \text{ord}(b))$.

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

Note that k may be 0, in which case $A(p) = \{0\}$, which is not interesting!

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 $\text{lcm}(\text{ord}(b), \text{ord}(b'))$. This last expression is a factor of m since both $\text{ord}(b)$ and $\text{ord}(b')$ 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 $p^s a$ has order t and ta has order p^s. Since $p \nmid t$ there are integers x, y such that $1 = xp^s + yt$. Then $a = (xp^s + yt)a = x(p^s a) + y(ta)$ can be expressed as a sum of an elment in $A(p)$ and one in B. □

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 $|A| = p_1^{e_1} \dots p_r^{e_r}$ 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 $\text{ord}(a) = qm$ then $\text{ord}(ma) = q$ so if any element has order divisible by q then there is an element of order q. Consequently, 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. □

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 (see Hungerford).

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 which has 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. □

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 $p_1^{e_1} \dots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

$$A(p_i) \cong \mathbb{Z}_{p_i^{a_{i,1}}} \times \mathbb{Z}_{p_i^{a_{i,2}}} \times \dots \mathbb{Z}_{p_i^{a_{i,s_i}}}$$

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.