Isomorphism theorems

Week of March 9, 2020

GU4041

Columbia University

March 12, 2020

Outline

Product of two subgroups

There are *three* isomorphism theorems, known by their numbers. First we need to define the notion of a *product of subgroups*.

Lemma

Let $J, N \subseteq G$ be two subgroups, with N normal in G (we write $N \trianglelefteq G$). Then the set

$$J \cdot N = \{j \cdot n,\ j \in J, n \in N\}$$

is a subgroup of G.

Proof.

It suffices to show that $J \cdot N$ is closed under multiplication and inverses . If $j \cdot n \in JN$, then

$$(jn)^{-1} = n^{-1}j^{-1} = j^{-1} \cdot (jnj^{-1}) \in J \cdot N$$

Proof.

Next, if $j_1, j_2 \in J$, $n_1, n_2 \in N$, then

$$(j_1 \cdot n_1)(j_2 \cdot n_2) = j_1 j_2 \cdot (j_2^{-1} n_1 j_2) n_2 \in J \cdot N,$$

again because N is normal. This completes the proof. □

First isomorphism theorem

Theorem

Let $f : G \to H$ be a homomorphism with kernel K. . Then there is an isomorphism

$$G/K = G/Ker(f) \xrightarrow{\sim} Image(f).$$

If G and H are vector spaces and f is a linear transformation, this can be compared to the formula

$$\dim G - \dim \ker(f) = \dim \ Image(f).$$

Second Isomorphism theorem

Theorem

Let G be a group, $H \subseteq G$ a subgroup, $N \trianglelefteq G$ a normal subgroup. Then the inclusion of H in $H \cdot N$ determines an isomorphism

$$H/H \cap N \xrightarrow{\sim} H \cdot N/N$$

Third isomorphism theorem

First recall that if $N \trianglelefteq G$ is a normal subgroup, then there is a bijection between the set S of subgroups of the quotient G/N and the set T of subgroups of G containing N.

If $\pi : G \to G/N$ is the quotient map, this correspondence is defined as follows: to each subgroup $J \subset G/N$, we associate the preimage $\pi^{-1}(J) \subset G$.

This defines a function from S to T. The inverse function takes a subgroup $H \subset G$ containing N to its image $\pi(H) \subset G/N$.

Third isomorphism theorem

Theorem

Let G be a group, $H \trianglelefteq G$, $N \trianglelefteq G$ two normal subgroups, with $N \subseteq H$. Then the natural homomorphism $G/N \to G/H$ induces an isomorphism

$$(G/N)/(H/N) \xrightarrow{\sim} G/H.$$

Proof of First Isomorphism Theorem

$$f : G \to H; \quad G/K = G/Ker(f) \xrightarrow{\sim} Image(f).$$

Proof.

Let $J = Image(f) \subset H$. Define $\alpha : G/K \to J$ by setting $\alpha(gK) = f(g)$.
First, α is *well-defined*; in other words, if $gK = g'K$ then $\alpha(gK) = \alpha(g'K)$. Now if $gK = g'K$ then $\exists k \in K$ such that $g' = gk$. Then

$$\alpha(gK) = f(g) = f(g) \cdot f(k) = f(gk) = f(g') = \alpha(g'K),$$

where the second equality follows because $f(k) = e$ for any $k \in \ker(f)$.

□

Proof of First Isomorphism Theorem

Proof.

Next, the image of α (which a priori is in H) is in fact contained in J. This is obvious by the definition of "image."

Third, α is surjective. Suppose $j \in J = Image(f)$. Thus there exists $g \in G$ such that $f(g) = j$. It follows that $\alpha(gK) = j$.

Finally α is injective. Suppose $\alpha(gK) = e$. Then $f(g) = e$, in other words $g \in \ker(f) = K$. So $gK = K$ which is the identity element of G/K. Thus α is injective. □

Proof of Second Isomorphism Theorem

Proof.

Consider the composition

$$H \hookrightarrow H \cdot N \to H \cdot N/N; \;\; h \mapsto h \cdot e_N \mapsto (h \cdot e_N)N \in H \cdot N/N.$$

Call the composition ϕ.

First, ϕ is *surjective*. Indeed, the map $\pi.H \cdot N \to H \cdot N/N$ is the surjective quotient map. Let $j \in H \cdot N/N$ and suppose $j = \pi(h \cdot n)$. Since $n \in N = \ker \pi$,

$$j = \pi(h \cdot n) = \pi(h) \cdot \pi(n) = \pi(h) = \pi(h \cdot e_N) = \phi(h).$$

Thus ϕ is surjective. □

Proof of Second Isomorphism Theorem

Proof.

Next,

$$\ker(\phi) = \{h \mid h \cdot e_N \in \ker(\pi)\} = \{h \mid h \cdot e_N \in N\}.$$

But $h \cdot e_N \in N$ if and only if $h \in N$. Since $h \in H$, it follows that $\ker(\phi) = H \cap N$. □

Proof of Third Isomorphism Theorem

Proof.

Let $\pi : G \to G/N$ be the quotient map. We define a homomorphism

$$f : G/N \to G/H; gN \mapsto gH.$$

This is well-defined because $N \subseteq H$: if $g'N = gN$ then $g'H = gH$. And it is a homomorphism because if $g_1, g_2 \in G$,

$$g_1 g_2 H = g_1 H \cdot g_2 H$$

because H is a normal subgroup. Moreover, f is surjective: if $j \in G/H$ then $j = gH$ for some $g \in G$, and then $j = f(gN)$. □

Proof of Third Isomorphism Theorem

Proof.

Finally,

$$\ker(f) = \{gN \mid gH = H\} = \{gN \mid g \in H\}$$

which is just $\pi(H)$. But $\pi(H) = H/N$ under the bijection between subgroups of G/N and subgroups of G containing N.
Thus $\ker(f) = H/N$. □

An example

Let $G = S_4$, $H = A_4 \supseteq N = K_4$. (We know N is normal in S_4 by a homework exercise.)
Then $H/N = A_4/K_4$ is a group of order 3, which must be the cyclic group $\mathbb{Z}_3$.

Question

$G/N = 6$. Is it isomorphic to $\mathbb{Z}_6$ or $S_3 = D_6$?

$\mathbb{Z}_6$ has an element of order 6. If $G/N = \mathbb{Z}_6$, then G must have an element of order at least 6. But S_4 has no such element. Thus $G/N = D_6$.
Of course $G/H = \mathbb{Z}_2$, H/N is the unique subgroup of order 3 in D_6, and $(G/N)/(H/N)$ is also $\mathbb{Z}_2$.
There are more interesting examples for finite abelian groups.

The main theorem

Theorem

Let A be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1, a_2, \ldots, a_n$$

(in no particular order) such that A is isomorphic to the direct product

$$A \xrightarrow{\sim} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=1}^{n} p_i^{a_i}.$$

Prime factors

This can be broken down into two theorems.

Theorem (Theorem 1)

Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct *primes dividing $|A|$, and say*

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Abelian groups of prime power order

Theorem (Theorem 2)

Let p be a prime and let A be a finite abelian group of order p^N for some $N > 1$. Then there is a sequence of positive integers $c_1 \leq c_2 \leq \cdots \leq c_s$ and an isomorphism

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_s}}.$$

Theorem 1 is essentially a series of applications of the Chinese Remainder Theorem, and is not very hard.

Theorem 2 is a more complicated induction argument.