Chapter 9 Isomorphisms.

We have previously talked loosely about two groups being "the same", but we used informal language and intuition to talk about a concept that should be rigorous.

Definition: Two groups are *isomorphic* if there is a bijection between them preserving the group operation. In symbols, if $(G, \cdot)$ and $(H, *)$ are groups, then they are *isomorphic* if there exists a bijection $\phi : G \longrightarrow H$ with

$$\phi(g_1 \cdot g_2) = \phi(g_1) * \phi(g_2) \text{ for all } g_1, g_2 \in G.$$

Example: The complex numbers $\{1, i, -1, -i\}$ form a group with complex multiplication as the operation. Define $\phi : \mathbb{Z}_4 \longrightarrow \{1, i, -1, -i\}$ by

$$\phi(n) = i^n.$$

Then $\phi(0) = 1$, $\phi(1) = i$, $\phi(2) = -1$, $\phi(3) = -i$, so it's a bijection. For any $m, n \in \mathbb{Z}_4$ we also have

$$\phi(m+n) = i^{m+n} = (i^m)(i^n) = \phi(m) \cdot \phi(n),$$

so the map preserves the group operation.

Thus $\mathbb{Z}_4$ and $\langle i \rangle < \mathbb{C}^*$ are *isomorphic*.

Example: Let $(\mathbb{R}^+, \cdot)$ denote the positive reals with multiplication, and $(\mathbb{R}, +)$ the reals with addition.
Then define $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ by $\phi(x) = e^x$.
We know e^x is bijective on these sets, but we also have

$$\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y),$$

so it is in fact an isomorphism.

Example: The permutation group S_3 has elements $\{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$, and we computed a while back that $\mu_1 \rho_1 \neq \rho_1 \mu_1$.
On the other hand, $\mathbb{Z}_6$ also has 6 elements, so it is possible to establish a bijection $\phi : \mathbb{Z}_6 \longrightarrow S_3$. However, this map cannot respect the group operation, here is why:
Let $a, b \in \mathbb{Z}_6$ be the elements satisfying

$$\phi(a) = \mu_1$$
$$\phi(b) = \rho_1,$$

these elements exist since ϕ is bijective. Now in order to respect the group operation, we need:

$$\begin{aligned} \phi(a+b) &= \phi(a)\phi(b) = \mu_1 \rho_1 \\ &\parallel \\ \phi(b+a) &= \phi(b)\phi(a) = \rho_1 \mu_1. \end{aligned}$$

But we know this equality is impossible since $\mu_1 \rho_1 \neq \rho_1 \mu_1$.

So $\mathbb{Z}_6$ and S_3 are not isomorphic.

Example: We saw the group

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

with addition defined by

$$(a,b) + (c,d) = (a+c, b+d).$$

It has 4 elements. The group $\mathbb{Z}_4$ also has 4 elements, so we can find a bijection $\phi: \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$.

Both groups are abelian, so if we want to investigate whether or not ϕ can preserve the group operation, we will need a more subtle argument than before.

So observe: • $1 \in \mathbb{Z}_4$ has order 4

• every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2.

This should give a problem!

Observe that, if $\phi: \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ then:

$$\phi(0) = \phi(0+0) = \underbrace{\phi(0) + \phi(0) = (0,0)}_{\text{because every element is order 2}}$$

and $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = (0,0)$,

and this contradicts ϕ being a bijection. So ϕ cannot be an isomorphism.

We can summarize some of these observations in a theorem.

Theorem: Suppose that $\phi: G \longrightarrow H$ is an isomorphism of groups. Then the following are true:

1) $\phi^{-1}: H \longrightarrow G$ is also an isomorphism

2) $|G| = |H|$

3) If G is abelian, then H is abelian

4) If G is cyclic, then H is cyclic

5) If G has a subgroup of order n, then H has a subgroup of order n.

6) If G has an element of order n, then H has an element of order n (follows from 5, more or less) but requires a bit more work.

Proof:

(1) and (2) are true because ϕ^{-1} exists, since ϕ is a bijection,

(3) Is proved as follows. Suppose G is abelian, and let $h_1, h_2 \in H$. Suppose $g_1, g_2 \in G$ satisfy $\phi(g_1) = h_1$, $\phi(g_2) = h_2$. Then

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1,$$

so H is abelian.

(4) Is proved this way: Let $G = \langle g \rangle$, and set $h = \phi(g)$. We will show $H = \langle h \rangle$, by showing that every $a \in H$ is a power of h.

Choose k so that $\phi(g^k) = a$. Then

$$a = \phi(g^k) = \phi(g)^k = h^k, \text{ so } H \text{ is cyclic.}$$

4, 5, 6 will be left as exercises.

Theorem: If G is a cyclic group with infinitely many elements, then G is isomorphic to $\mathbb{Z}$.

Proof: Let $G = \langle g \rangle$, if G is infinite then g has infinite order, so $G = \{\dots g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$.

So define $\phi: \mathbb{Z} \longrightarrow G$ by $\phi(n) = g^n$. Then

$$\phi(m+n) = g^{m+n} = g^m \cdot g^n = \phi(m) \cdot \phi(n),$$

so ϕ is an isomorphism.

Technically, we must also show injectivity, so suppose $\phi(n) = \phi(m)$ for $m \neq n$, Then say $m > n$.

$\phi(n) = g^n = \phi(m) = g^m$. Therefore

$$g^{m-n} = e \quad \text{where } m-n > 0.$$

This means g has finite order, a contradiction.

Surjectivity is easy, since G is cyclic every element is of the form g^n for some n.

Theorem: If G is a cyclic group of order n, then G is isomorphic to $\mathbb{Z}_n$.

Proof: If $G = \langle g \rangle$ is of order n, define

$$\phi(g^m) = m \quad \text{for} \quad 0 \leq m \leq n-1.$$

Then check that this is an isomorphism.

Corollary: If G is a group and $|G| = p$, where p is prime, then G is isomorphic to $\mathbb{Z}_p$.

Proof: We already saw that $|G| = p$ implies that G is cyclic, so from there we need only apply the previous theorem.

Remark: From now on, we consider two groups to be "the same" if they are isomorphic. Precisely, isomorphism of groups determines an equivalence relation on the set of all groups, and we'll consider two groups to be "the same" if they are in the same equivalence class.

One of the reasons that permutation groups are so significant is that they provide a "universal" kind of group, in the following sense:

Theorem (Cayley).
Every group is isomorphic to a group of permutations.

Proof: Let G be an arbitrary group. We will create a second group $\overline{G}$ which is a group of permutations isomorphic to G.

To create a group of permutations we require a set of elements that we'll permute, so take G as our set.

Define a function $\lambda_g : G \longrightarrow G$ for each $g \in G$ by

$$\lambda_g(h) = gh.$$

First, we check λ_g is 1-1 and onto. To see it's 1-1, suppose $\lambda_g(h) = \lambda_g(h')$.
Then $gh = gh'$, which implies $h = h'$ by left cancelation.
So λ_g is injective. To see it's surjective, let $h \in G$ be given. Then $\lambda_g(g^{-1}h) = g(g^{-1}h) = h$, so λ_g is surjective. Therefore λ_g is a permutation of the set of elements of G.

Define $\bar{G} = \{\lambda_g \mid g \in G\}$. Then $\bar{G}$ is a group of permutations of the elements of G (check this!).
We can define a map $\phi : G \longrightarrow \bar{G}$ by $\phi(g) = \lambda_g$, and check that ϕ in fact gives an isomorphism.

First notice that the group operation is preserved, since

$$\phi(gh) = \lambda_{gh} \quad \text{and} \quad \phi(g)\phi(h) = \lambda_g \cdot \lambda_h,$$

and given an element $f \in G$, the maps λ_{gh} and $\lambda_g \circ \lambda_h$ act on it in the same way:

$$\lambda_{gh}(f) = ghf, \quad \lambda_g \circ \lambda_h(f) = \lambda_g(hf) = ghf.$$

Moreover, the map is one-to-one since

$$\phi(g) = \phi(h) \text{ implies } \lambda_g(a) = \lambda_h(a) \text{ for all } a.$$

In particular $\lambda_g(e) = g \cdot e = g$ is equal to

$$\lambda_h(e) = h \cdot e = h, \text{ so } g = h \text{ and } \phi \text{ is injective.}$$

Finally, ϕ is surjective since $\overline{G}$ consists exactly of permutations of the form λ_g for some $g \in G$, each of which is the image of some $g \in G$ (by definition).

Next we explore ways to make new groups from old ones. This topic is split into two parts, some at the end of Chapter 9 and some in Chapter 10.

In Chapter 9 we have:

Direct Products

There are two flavours of direct product, the internal and external direct products of groups.

Definition: Suppose $(G, \circ)$ and $(H, *)$ are groups. Define a binary operation on the set of pairs

$$G \times H = \{(g, h) \mid g \in G \text{ and } H \ni h\}$$

according to the rule:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$$

$\circ$: group operation from G

$*$: group operation from H.

This makes $G \times H$ into a group, called the external direct product of G and H.

Proposition: If G and H are groups, then the set $G \times H$ with the operation given above does indeed form a group.

Proof: We check 4 things:

(i) The rule gives a binary operation $(G \times H) \times (G \times H) \to G \times H$ since any product

$$(g_1, h_1) \cdot (g_2, h_2)$$

gives an output with an element of G in the first coordinate, and an element of H in the second.

(ii) If e_G and e_H are identities in G and H respectively, then $(e_G, e_H) \in G \times H$ serves as an identity.

(iii) If $(g, h) \in G \times H$ then (g^{-1}, h^{-1}) is the inverse.

(iv) The operation is associative since the operations on G and H are associative.

Examples: The group $\mathbb{Z}_2 \times \mathbb{Z}_2$, which we already encountered, is an example of this, we saw it has 4 elements but is different from $\mathbb{Z}_4$.

Consider $\mathbb{Z}_2 \times \mathbb{Z}_3$, and what happens if we iterate the group operation applied to $(1,1)$.

$(0,0)$, $(1,1)$, $(0,2)$, $(1,0)$, $(0,1)$, $(1,2)$, and that's all of them. So in $\mathbb{Z}_2 \times \mathbb{Z}_3$, a group with 6 elements, we found $(1,1)$ has order 6! Thus

$\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic of order 6, ie.

$\mathbb{Z}_3 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$.

Theorem: Let $(g,h) \in G \times H$ be given. If g and h have finite orders in G and H respectively, then the order of (g,h) in $G \times H$ is $\text{lcm}(|g|, |h|)$.

Proof: Suppose g has order r and h has order s, and let m denote their least common multiple. Set $n = |(g,h)|$, we'll show $n=m$.

First note that since

$$(g,h)^m = (g^m, h^m) = (e_G, e_H),$$

we know that n must divide m. Second, since

$$(g^n, h^n) = (g,h)^n = (e_G, e_H),$$

we know that r and s both must divide n, so n is a common multiple of r and s. Thus m divides n, since m is the least common multiple. Thus $n=m$.

$\square$

Theorem: If $G_1, G_2, \ldots, G_k$ are groups and $g_i \in G_i$ for $i=1,\ldots,k$, then the order of $(g_1, \ldots, g_k) \in G_1 \times \ldots \times G_k$ is determined by induction. That is, if g_i has order r_i then the order of $(g_1, \ldots, g_k)$ is $\text{lcm}(r_1, \ldots, r_k)$.

Corollary: The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m,n)=1$.

Proof: First suppose $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, we'll show that $\gcd(m,n)=1$ by proving the contrapositive. If $\gcd(m,n)>1$, say $\gcd(m,n)=d$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic, and here is why: The number $\frac{mn}{d}$ is divisible by both m and n, so for any $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ we have

$$\underbrace{(a,b)+(a,b)+\dots+(a,b)}_{\frac{mn}{d} \text{ terms}} = (0,0).$$

But this means no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ can have order $mn > \frac{mn}{d}$, so $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic. Conversely, if $\gcd(m,n)=1$, then $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ has order mn by the previous theorem, so $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (1,1) \rangle$.

Similar to the theorem, the corollary also has generalizations to higher-order products, ie to groups $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$.

The construction of an external direct product takes groups G, H and makes a new one $G \times H$ out of them.

An internal direct product is when we take a group, and show that it is actually the external direct product of its subgroups, as follows:

Definition: Let $H, K \subset G$ be subgroups of the group G. If:

- $HK = \{hk \mid h \in H, k \in K\} = G$
- $H \cap K = \{e\}$
- $hk = kh \quad \forall h \in H$ and $k \in K$

then G is the internal direct product of H and K.

Example: The group $\mathbb{Z}_6$ has subgroups $H = \{0, 2, 4\}$ and $\{0, 3\} = K$. They satisfy the required properties, so $\mathbb{Z}_6$ is the internal direct product of H & K.

Theorem: If G is the internal direct product of H and K then G is isomorphic to $H \times K$.

Proof: Define a map $\phi: H \times K \longrightarrow G$ by $\phi(h,k) = hk$.

Then ϕ is surjective, since every element of G can be written as hk (G is internal direct product).

Also ϕ is injective, for if

$$\phi(h_1, k_1) = \phi(h_2, k_2)$$

$$\Rightarrow h_1 k_1 = h_2 k_2$$

$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1}.$$

But this means an element of H is equal to an element of K, since $H \cap K = \{e\}$ this forces $h_2^{-1} h_1 = e$ and $k_2 k_1^{-1} = e \Leftrightarrow (h_1, k_1) = (h_2, k_2)$.

Last, ϕ preserves the group operation:

$$\phi((h_1, k_1)(h_2, k_2)) = \phi((h_1 h_2, k_1 k_2))$$

$$= h_1 h_2 k_1 k_2$$

$$= h_1 k_1 h_2 k_2 \quad \text{since elts of } H \text{ commute with elts of } K$$

$$= \phi((h_1, k_1)) \cdot \phi(h_2, k_2).$$

Chapter 9

1-5, 8-10, 18-23, 31, 34