ITC8190
Mathematics for Computer Science
Group Isomorphisms

Aleksandr Lenin

December 11th, 2018

Table: Cayley tables for $U(8)$ and $U(12)$

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Many groups may appear to be different at first glance, but can be shown to be the same by simple renaming of the group elements.

$$1 \mapsto 1, \qquad 3 \mapsto 5, \qquad 5 \mapsto 7, \qquad 7 \mapsto 11$$

In such a case we say that groups are **isomorphic**.

Two groups $(G, \otimes)$ and $(H, \circ)$ are **isomorphic** if there exists a bijection $\phi : G \to H$ such that the group operation is preserved

$$\phi(a \otimes b) = \phi(a) \circ \phi(b) \ .$$

for all $a, b \in G$.

If G is isomorphic to H, we write $G \cong H$, and the map ϕ is called an **isomorphism**.

Example 1

Let us show that $\mathbb{Z}_4 \cong \langle i \rangle$, where $\langle i \rangle = \{i, -1, -i, 1\}$ is the group of 4-th roots of unity. Define a map $\phi : \mathbb{Z}_4 \to \langle i \rangle$ by $\phi : n \mapsto i^n$. The inverse map $\psi : \langle i \rangle \to \mathbb{Z}_n$ is given by $\psi : i^n \mapsto n$.

The map $\phi : \mathbb{Z}_n \to \langle i \rangle$ is a bijection, since

$$(\psi \circ \phi)(n) = \psi(i^n) = n \ ,$$
$$(\phi \circ \psi)(i^n) = \phi(n) = i^n \ .$$

To show that ϕ is an isomorphism, observe that for all $a, b \in \mathbb{Z}_n : \phi(a + b) = i^{a+b} = i^a \cdot i^b = \phi(a) \cdot \phi(b)$. Hence, $(\mathbb{Z}_4, +) \cong (\langle i \rangle, \cdot)$.

Example 2

The groups $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$ cannot be isomorphic, since their orders are different. However $U(8) \cong U(12)$ as was shown in the first slide.

In fact, both of these groups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Table: Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Abelian and nonabelian groups cannot be isomorphic.

Example 3

Even though the group of symmetries S_3 and $\mathbb{Z}_6$ contain the same number of elements, they are not isomorphic because $\mathbb{Z}_6$ is abelian and S_3 is nonabelian.

To demonstrate that this is the case, suppose that $\phi : \mathbb{Z}_6 \to S_3$ is an isomorphism. Let $a, b \in S_3$ and $ab \neq ba$. Since ϕ is an isomorphism, there exist $m, n \in \mathbb{Z}_6$ such that $\phi(m) = a$ and $\phi(n) = b$. However,

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba \ ,$$

which contradicts the fact that a and b do not commute.

Let $\phi : G \to H$ be isomorphism of two groups. Then the following statements are true:

1. $\phi^{-1} : H \to G$ is 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.

Theorem 1

All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.

Proof.

Let G be a cyclic group with infinite order and suppose that $G = \langle a \rangle$. Define a map $\phi : \mathbb{Z} \to G$ by $\phi : n \mapsto a^n$. Then

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n) \ .$$

It can be seen that ϕ is surjective, since any element in G can be written as a^n for some integer n and $\phi(n) = a^n$. ϕ is injective, since $a^m = a^n \implies m = n$. Hence, ϕ is a bijection. □

Theorem 2

If G is a cyclic group of order n, then $G \cong \mathbb{Z}_n$.

Proof.

Let G be a cyclic group of order n generated by a and define a map $\varphi : \mathbb{Z}_n \to G$ by $\varphi : k \mapsto a^k$, where $0 \leqslant k \leqslant n$. Define an inverse map $\psi : G \to \mathbb{Z}_n$ by $\psi : x \mapsto n : x = a^n$. Then

$$(\psi \circ \varphi)(x) = \psi(n) = a^n = x \ ,$$
$$(\varphi \circ \psi)(x) = \phi(a^x) = x \ .$$

Hence, φ is a bijection. To show that φ is an isomorphism, observe that it preserves group operations,

$$\varphi(x + y) = a^{x+y} = a^x \cdot a^y = \varphi(a) \cdot \varphi(b) \ .$$

Hence, $G \cong \mathbb{Z}_n$. □

Theorem 3

The isomorphism of groups determines an equivalence relation on the class of all groups.

$$G \sim H \Longleftrightarrow G \cong H \ .$$

Proof.

We can show that the isomorphism is an equivalence relation. It is clearly reflexive $G \cong G$, it is symmetric $G \cong H \implies H \cong G$, and transitive $G \cong H, H \cong T \implies G \cong T$. Hence, isomorphism is an equivalence relation on the class of all groups. □

The main goal of group theory is to classify all groups. However, it makes sense to consider to groups to be the same if they are isomorphic.

Hence, the main goal of group theory is to classify all groups **up to an isomorphism**.

One important theorem in group theory is the Cayley theorem.

Theorem 4 (Cayley)

Every group is isomorphic to a group of permutations.

Proof.

Omitted, since this course does not cover the topic of permutation groups. □

Definition 1 (External Direct Product)

If $(G, \odot)$ and $(H, \circ)$ are groups, then their Cartesian product is a group $(G \times H, \bullet)$ under operation

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \odot g_2, h_1 \circ h_2) \ .$$

The group $G \times H$ is called the **external direct product** of G and H.

For the sake of clarity we write

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

We may compose the direct product of more than just 2

groups:

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n \ .$$

Example 4

The group $(\mathbb{R}, +)$ is the group of real numbers under addition. The Cartesian product $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is also a group, in which the group operation is

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

the identity is $(0, 0)$, and the inverse of every element (a, b) is $(-a, -b)$.

Consider

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

Although $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ both contain 4 elements, it is easy to see that they are not isomorphic, since for every element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, $(a, b) + (a, b) = (0, 0)$, but $\mathbb{Z}_4$ is cyclic.

Unlike that of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, it is true that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. We only need to show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is easy to see that $(1, 1)$ generates $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Theorem 5

Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) in $G \times H$ is the least common multiple of r and s.

Proof.

Suppose that m is the least common multiple of r and s, and let $n = |(g, h)|$. Then

$$(g, h)^m = (g^m, h^m) = (e_G, e_H) \ , \quad (g, h)^n = (g^n, h^n) = (e_G, e_H) \ .$$

By the first equation, m must be a multiple of n, since n is the least integer such that $(g, h)^n = (e_G, e_H)$ by definition of the order of element in a group. And so, $n \leqslant m$. However, by the second equation, both r and s must divide n, therefore n is a common multiple of r and s. Since m is the least common multiple of r and s, $m \leqslant n$. Consequently, $m = n$. □

Theorem 6

$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ *iff* $\gcd(m, n) = 1$.

Proof.

First, we show that $\gcd(m, n) = d > 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic. Since mn/d is a multiple of both m and n, for any element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a, b) + (a, b) + \ldots + (a, b)}_{mn/d \text{ times}} = (0, 0) \ .$$

Therefore, no (a, b) can generate all of $\mathbb{Z}_m \times \mathbb{Z}_n$, and hence if $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, then $\gcd(m, n) = 1$.

Assume now that $\gcd(m, n) = 1$. If $|a| = m$ and $|b| = n$, then by Theorem 5, $|(a, b)| = \operatorname{lcm}(m, n) = mn$, and it generates $\mathbb{Z}_m \times \mathbb{Z}_n$. Hence, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. □

Theorem 7

Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$, where $g_1, g_2 \in G$ and $h_1 h_2 \in H$.

Proof.

By closure of group operations in G and H, clearly the operation defined above is closed. The associativity of this operation follows from the associativity of operations in G and H. If e_G and e_H are identities in G and H, then (e_g, e_H) is the identity in $G \times H$. The inverse of $(g, h) \in G \times H$ is $(g, h)^{-1} = (g^{-1}, h^{-1})$. □

From Theorem 7 it follows that

Corollary 1

Let $n_1, \ldots, n_k$ be positive integers. Then

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

iff $\gcd(n_i, n_j) = 1$ *for* $i \neq j$*.*

Corollary 2

If $m = p_1^{e_1} \cdots p_k^{e_k}$ *where* $p_i s$ *are distinct primes, then*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}} \ .$$

Proof.

Since $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$ for $i \neq j$, the proof follows from Corollary 1. □

Definition 2 (Internal Direct Product)

Let G be a group with subgroups H and K satisfying the following conditions

1. $G = HK = \{hk : h \in H, k \in K\}$
2. $H \cap K = \{e\}$
3. H and K are **normal** subgroups, i.e., $hk = kh$ for all $k \in K$ and $h \in H$

Then G is the **internal direct product** of H and K.

Example 5

The group $U(8)$ is the external direct product of $H = \{1, 3\}$ and $K = \{1, 5\}$.

Theorem 8

Let G be the internal direct product of subgroups H and K. Then $G \cong H \times K$.

Proof.

Since G is an internal direct product, we can write every element $g \in G$ as $g = hk$ for some $h \in H$ and some $k \in K$. Define a map $\phi : G \to H \times K$ by $\phi(g) = (h, k)$.
First, we need to show that ϕ is a well-defined map, that is, h and k are uniquely determined by g. Suppose that $g = hk = h'k'$. Then $h^{-1}h' = k(k')^{-1}$ in both H and K, so it must be the identity, since the inner direct product requires that $H \cap K = \{e\}$. Therefore, $h = h'$ and $k = k'$ which proves that ϕ is indeed well-defined.

The proof continues in the next slide...

Theorem 8

Let G be the internal direct product of subgroups H and K. Then $G \cong H \times K$.

Proof.

To show that ϕ preserves the group operation, let $g_1 = h_1 k_1$, and $g_2 = h_2 k_2$. Then

$$\begin{aligned}
\phi(g_1 g_2) &= \phi(h_1 k_1 h_2 k_2) \\
&= \phi(h_1 h_2 k_1 k_2) \\
&= (h_1 h_2, k_1 k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \phi(g_1)\phi(g_2) \quad .
\end{aligned}$$

The proof continues on the next slide...

Theorem 8

Let G be the internal direct product of subgroups H and K. Then $G \cong H \times K$.

Proof.

Define an inverse map $\phi^{-1} : H \times K \to G$ by $\phi : (h, k) \mapsto g$, where $g = hk$.

$$(\phi^{-1} \circ \phi)(g) = \phi^{-1}(h, k) = g \ \ ,$$
$$(\phi \circ \phi^{-1})(h, k) = \phi(g) = (h, k) \ \ .$$

Hence, ϕ is a bijection and since it preserves the group operation, it is an isomorphism. □

?

THANK YOU
FOR
YOUR
ATTENTION
ANY QUESTIONS?