

Pseudomorphisms and Order Equivalence of Groups

In group theory, an isomorphism is a bijection $\varphi : G \rightarrow G'$, such that $\forall g_1, g_2 \in G, \varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$. From this, we can deduce that an isomorphism between two groups forces the groups to be *order equivalent*.

Definition: Order Equivalent

Two groups are order equivalent if:

- 1) both groups are of the same order, and
- 2) both groups contain elements with corresponding orders; hence there exists a bijection, $\phi : G \rightarrow G'$ such that $\forall g \in G, |g| = |\phi(g)|$.

For example, if we have \mathbb{Z}_4 , we know it is not isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, because \mathbb{Z}_4 contains an element of order 4 and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ does not.

This argument will focus on the converse of the above statement and its application to finite groups. That is, if we know that two finite groups are order equivalent, are they necessarily isomorphic? And, if so, is this true for all finite groups?

The first question, which asks are two order equivalent, finite groups necessarily isomorphic, is proved false by the following counterexample. This counterexample, provided by Joseph Gallian, and its proof verify that the statement is false in general.

Gallian Counterexample:

Let $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $G' = M_3^\Delta(\mathbb{Z}_3)$, where $M_3^\Delta(\mathbb{Z}_3)$ is the group of 3×3 upper triangular matrices with \mathbb{Z}_3 coefficients,

$$\text{i.e. } M_3^\Delta(\mathbb{Z}_3) = \left\{ \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix} \mid \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_3 \right\}.$$

Gallian claims that these two groups, although order equivalent, are not isomorphic.

Proposition 1:

$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ is order equivalent, but not isomorphic to $M_3^\Delta(\mathbb{Z}_3)$, where $M_3^\Delta(\mathbb{Z}_3)$ is the group of 3×3 upper triangular matrices with \mathbb{Z}_3 coefficients.

PROOF:

First, we can show that G and G' are order equivalent.

Since, G is a direct product, its order is the product of each factor's order; so, we have $3 \cdot 3 \cdot 3$, or $|G| = 27$. $|G'|$ can be determined by looking at a generic matrix from $M_3^\Delta(\mathbb{Z}_3)$.

Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_3$, then a matrix in $M_3^\Delta(\mathbb{Z}_3)$ looks like:

$$\begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix}$$

where \bar{a} , \bar{b} , and \bar{c} each have three possible values: $\bar{0}, \bar{1}, \bar{2}$. Since each variable has three possible values and there are three variables, we have that $|G'| = 3^3 = 27$.

Therefore, $|G| = |G'| = 27$.

Next, we are to verify that G and G' contain elements of corresponding orders. We know that in $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, all elements are of order 3 except for the identity $(0, 0, 0)$, which has order 1. We know this from Theorem 8.1 (Gallian, 151), which states that the order of an element in a direct product is the least common multiple of the orders of the components of the element. The following lemma proves that all elements of $M_3^\Delta(\mathbb{Z}_3)$ are also of order 3, except for the identity matrix, whose order is 1.

Lemma 1:

The order of an element in $M_3^\Delta(\mathbb{Z}_3)$ is either 1 or 3.

PROOF:

We can see this is true by cubing a generic matrix from $M_3^\Delta(\mathbb{Z}_3)$. Performing the matrix multiplication, we have:

$$\begin{aligned} \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix}^3 &= \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & \bar{a} & \bar{b} \\ 0 & 1 & \bar{c} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2\bar{a} & 2\bar{b} + 2\bar{a}\bar{c} \\ 0 & 1 & 2\bar{c} \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 3\bar{a} & 3\bar{b} + 3\bar{a}\bar{c} \\ 0 & 1 & 3\bar{c} \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$

If we examine the case where $\bar{a}, \bar{b}, \bar{c} = 0$, the generic matrix reduces to the identity matrix. We notice that by cubing the generic matrix, a factor of 3 is introduced to each variable entry. Thus, $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_3, \bar{a}, \bar{b}, \bar{c} \neq 0$, the entries in the upper corner of the matrix reduce to 0 modulo 3 to form the identity matrix. This tells us that the order of any element in $M_3^\Delta(\mathbb{Z}_3)$ is either 1 or 3. We know that the only element of order 1 is the identity. Therefore, for any $\bar{a}, \bar{b}, \bar{c} \neq 0$ we choose, the order of the resulting element is 3. \square

Quoting the above Lemma, we can now show that $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $M_3^\Delta(\mathbb{Z}_3)$ both have 1 element of order 1, and 26 elements of order 3. Combining this with the fact that $|G| = |G'| = 27$, we have shown that $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $M_3^\Delta(\mathbb{Z}_3)$ are order equivalent.

Now that we have verified that, in fact, G and G' are order equivalent, we must show that they are not isomorphic. This task is simplified by the manner in which we chose our groups, G and G' . $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ is Abelian

because each factor is Abelian, but $M_3^\Delta(\mathbb{Z}_3)$ is not Abelian. For example, the following matrices do not commute:

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

This implies $M_3^\Delta(\mathbb{Z}_3)$ is non-Abelian. In fact, these matrices will not commute for all $M_3^\Delta(\mathbb{Z}_n)$. So, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \not\cong M_3^\Delta(\mathbb{Z}_3)$, because the latter is not Abelian. But, these groups are order equivalent. ■

This leads to a definition.

Definition: Pseudomorphism

G and G' are pseudomorphic if $G \not\cong G'$, but G and G' are order equivalent. That is, there exists a bijection $\varrho : G \rightarrow G'$, such that $\forall g \in G, |g| = |\varrho(g)|$, but $\exists g_1, g_2 \in G$, such that $\varrho(g_1 \cdot g_2) \neq \varrho(g_1) \circ \varrho(g_2)$.

We have shown that two groups, although order equivalent, are not necessarily isomorphic. This raises the question as to what orders, other than 27, can have two groups of that order be pseudomorphic. This question is addressed later by a generalization of Proposition 1. First, in order to simplify our work, we will need another definition.

Definition: Order Determined

An integer n is order determined if and only if any two groups of order n which are order equivalent must be isomorphic. Stated using our definitions we have, n is order determined if and only if there *does not* exist a pseudomorphism between two groups of order n .

Note: We have shown that $n = 27$ is *not* order determined. Gallian asserts that $n = 27$ is the first occurrence of a group order that is not order determined. We will accept this as true and only concern this argument with looking at orders where $n > 27$.

We can now use Proposition 1 to generate a family of examples of group which will allow us to find integers, greater than 27, which are not order determined. For instance, if we can show that raising our generic matrix in $M_3^\Delta(\mathbb{Z}_k)$ to the k th power reduces to the identity matrix, modulo k , we can follow the same line of argument as in Proposition 1, and show that $M_3^\Delta(\mathbb{Z}_k)$ is pseudomorphic to $\mathbb{Z}_k \oplus \mathbb{Z}_k \oplus \mathbb{Z}_k$.

The first step in verifying when this generalization will produce two groups that are pseudomorphic is observing the behavior of a general matrix in $M_3^\Delta(\mathbb{Z}_k)$ when raised to the k th power. Properties of modular arithmetic allow us to calculate the matrix to the k th power with integer values for a , b , and c , and then reduce the entries of the resulting matrix modulo k . This brings us to another Lemma.

Lemma 2:

Let $M \in M_3^\Delta(\mathbb{Z})$. Then,

$$M^k = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{bmatrix}$$

PROOF:

We will prove this inductively, using Proposition 1 as our base case ($k = 3$). We begin by assuming our conjectured formula for M^k to be true, and use it to show that:

$$M^{k+1} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & (k+1)a & (k+1)b + \frac{k(k+1)}{2}ac \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{bmatrix}$$

We can proceed by noticing that:

$$\begin{aligned}
\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{k+1} &= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^k \\
&= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & (k+1)a & (k+1)b + \frac{k(k+1)}{2}ac \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}$$

This is what we were trying to prove; therefore, verified by induction, the formula for M^k is true $\forall k \geq 3$. \square

So, we have found a valid general formula for an $M \in M_3^\Delta(\mathbb{Z})$ raised to the k th power. We can now use this formula to find which values of k will make each respective group of matrices have all of its elements to the k th power reduce to the identity matrix modulo k . For these values of k , the corresponding elements of these matrix groups will all have order k (except for the identity), which allows the application of the same argument used in Proposition 1.

We have proved in Proposition 1 that by using the $k = 3$ case, we have that $n = 27$ is non-order determined. After observing what happens when $k > 3$, we find that only odd values of k force M^k to reduce to the identity matrix modulo k . Due to the complexity associated with groups of higher composite order, we will restrict this argument to the primes, a subset of the odd numbers that are greater than 3. This will aid in calculating the orders of all the elements, and guarantee that the direct product we need later in our argument, $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$, is order equivalent to $M_3^\Delta(\mathbb{Z}_p)$.

Proposition 2:

$M_3^\Delta(\mathbb{Z}_p)$, where p is a prime greater than 3, is pseudomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Equivalently, proving this will also show that p^3 is not order determined.

PROOF:

Let $M \in M_3^\Delta(\mathbb{Z}_p)$.

$$\text{Then, by Lemma 2, } M^p = \begin{bmatrix} \bar{1} & p\bar{a} & p\bar{b} + \frac{p(p-1)}{2}\bar{a}\bar{c} \\ \bar{0} & \bar{1} & p\bar{c} \\ \bar{0} & \bar{0} & \bar{1} \end{bmatrix}.$$

We can see that the coefficients of \bar{a} , \bar{b} , and \bar{c} are all multiples of p , and consequently reduce to 0 modulo p . Knowing this, we need only show that the coefficient of $\bar{a}\bar{c}$ also reduces to 0 modulo p , to force M^p to be the identity matrix.

By assumption, p is a prime greater than 3, therefore p is of the form $2q + 1$. It then follows that:

$$\begin{aligned} \frac{p(p-1)}{2} &= \frac{(2q+1)2q}{2} \\ &= (2q+1)q \\ &= pq \end{aligned}$$

Therefore, $\frac{p(p-1)}{2}$ is a multiple of p , hence 0 modulo p . This proves that M^p reduces to the identity matrix modulo p , and that all the elements in $M_3^\Delta(\mathbb{Z}_p)$ have order p except for the identity (extension of Lemma 1). This is enough information to reason similarly to Proposition 1, and prove that $M_3^\Delta(\mathbb{Z}_p)$ is pseudomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Consequently, in proving this, we have also shown that p^3 , $\forall p > 3$ is not order determined. ■