MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Mon, Mar 30, 2020

Chapter 8; External Direct Products

Let $G_1, G_2, \cdots G_n$ be a finite collection of groups. First consider their Cartesian product

$$G_1 \times G_2 \times \cdots \times G_n = \{ (g_1, g_2, \cdots, g_n) \mid g_i \in G_i, i = 1, 2, \cdots n \} \quad (1)$$

These are all possible ordered n-tuples, where the i^{th} member of the n-tuple is a member of the i^{th} group G_i in the listing given above, and with equality defined by

$$(g_1, g_2, \cdots, g_n) = (g_1', g_2', \cdots, g_n') \text{ iff } g_i = g_i' \text{ for } i = 1, 2, \cdots n \quad (2).$$

This is just the standard definition of the Cartesian product of G_i treated as sets. However since each G_i is a group, we can provide a group structure on the Cartesian product by defining

$$(g_1, g_2, \cdots, g_n) \cdot (g_1', g_2', \cdots, g_n') = (g_1 g_1', g_2 g_2', \cdots, g_n g_n'), \quad (3)$$

where $g_i g_i'$ is the "product" defined by the group operation in G_i.

In the book, the notation $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is used instead of (1), for the Cartesian product endowed with the operation defined in (3). Other authors retain the notation of the Cartesian product, which is natural, but in order to avoid confusion, we will discard the notation in (1) and use $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ instead. We begin with

Theorem 1: The set $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is a group with the coordinatewise multiplication operation defined in (3). This is called the External Direct Product of the G_i.

Proof: The two n-tuples on the left in (3) are elements of $G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Since for each i, the product $g_i g_i' \in G_i$, the n-tuple on the right in (3) is an element of $G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Hence the operation defined in (3) is a closed binary operation on $G_1 \oplus G_2 \oplus \cdots \oplus G_n$. This operation can similarly be shown to be associative.

Next if $e_1, e_2, \cdots, e_n$ denote the identity elements of $G_1, G_2, \cdots, G_n$ respectively, then $(e_1, e_2, \cdots, e_n)$ is the identity element for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$

as can be seen from (3). Finally with $e=(e_1, e_2, \cdots, e_n)$ as the identity (2)
in $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, we see that the inverse of $(g_1, g_2, \cdots, g_n)$ is

$$(g_1, g_2, \cdots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1})$$

because

$$\left.\begin{aligned} &(g_1, g_2, \cdots, g_n)\cdot(g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}) = (g_1 g_1^{-1}, g_2 g_2^{-1}, \cdots, g_n g_n^{-1}) = (e_1, e_2, \cdots, e_n) \\ \& \quad &(g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1})\cdot(g_1, g_2, \cdots, g_n) = (g_1^{-1} g_1, g_2^{-1} g_2, \cdots, g_n^{-1} g_n) = (e_1, e_2, \cdots, e_n) \end{aligned}\right\} \quad (4)$$

This proves Theorem 1.

Note that if each G_i is finite

$$|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1|\,|G_2| \cdots |G_n| \qquad (5)$$

because this equality on size holds for Cartesian products. Equation (5) also holds if any of the G_i ~~are~~ is infinite in size.

Next we prove

Theorem 8.1 : (Order of an element in an External Direct Product)

Let $G_1, G_2, \cdots, G_n$ be a collection of finite groups. Let $(g_1, g_2, \cdots, g_n) \in G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Then the order of $(g_1, g_2, \cdots, g_n)$ in $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is given by

$$|(g_1, g_2, \cdots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \cdots, |g_n|).$$

Proof: Let e_i denote the ~~elem~~ identity element of G_i, for $i=1, 2, \cdots, n$. Let $t_i = |g_i|$ and $t = |(g_1, g_2, \cdots, g_n)|$. Put $s = \operatorname{lcm}(|g_1|, |g_2|, \cdots, |g_n|)$
$= \operatorname{lcm}(t_1, t_2, \cdots, t_n)$.

Since $t_i \mid s$, for each i, we have $g_i^s = e_i$ for $i=1, 2, \cdots, n$. Thus

$$(g_1, g_2, \cdots, g_n)^s = (g_1^s, g_2^s, \cdots, g_n^s) = (e_1, e_2, \cdots, e_n).$$

Thus $t \leq s$ (indeed $t \mid s$).

Next since $t = |(g_1, g_2, \cdots, g_n)|$, we have

$$(g_1, g_2, \cdots, g_n)^t = (g_1^t, g_2^t, \cdots, g_n^t) = (e_1, e_2, \cdots, e_n)$$

and so

$$g_i^t = e_i \quad \text{for} \quad i = 1, 2, \cdots, n.$$

This means that

$$|g_i| \mid t, \quad \text{for } i = 1, 2, \cdots, n$$

and so

$$t \geq \operatorname{lcm}(|g_1|, |g_2|, \cdots, |g_n|) = s$$

indeed $\operatorname{lcm}(|g_1|, |g_2|, \cdots, |g_n|) = s \mid t$.

Thus $s = t$ which is the assertion of the theorem.

—

An Example

The groups $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4$ although of the same size are not isomorphic.

Note that

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

where (by abuse of notation), we have written 0 for $[0]_2$ and 1 for $[1]_2$.

Note that $|(0,0)| = 1$, since $(0,0)$ is the identity and that

$$|(0,1)| = |(1,0)| = |(1,1)| = 2.$$

That is all non-identity elements have order 2.

On the other hand, $\mathbb{Z}_4$ is cyclic of order 4, and has two generators: $\mathbb{Z}_4 = \langle [1]_4 \rangle = \langle [3]_4 \rangle$. Thus by just considering orders, we see that $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic.

One could consider a map between $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4$ using binary representation.

$(0,0) \leftrightarrow 0$, $(0,1) \leftrightarrow 1$, $(1,0) \leftrightarrow 2$, $(1,1) \leftrightarrow 3$.

But this map is not operation preserving.

There are however some instances when $\mathbb{Z}_m \oplus \mathbb{Z}_n$ will be isomorphic to $\mathbb{Z}_{mn}$. This is given by the next theorem.

Theorem 8.2: Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime, that is $\gcd(|G|, |H|) = 1$.

Proof: Let $|G| = m$ and $|H| = n$. Then $|G \oplus H| = mn$.

($\Rightarrow$) Suppose $G \oplus H$ is cyclic. Then $G \oplus H = \langle (g,h) \rangle$, where $|(g,h)| = mn$. Suppose m & n are not relatively prime. This means ~~$\gcd(m,n) = d > 1$~~

$$\gcd(m,n) = d > 1.$$

Thus

$$\operatorname{lcm}(m,n) = \frac{mn}{d} < mn. \qquad (6)$$

But then

$$|(g,h)| = \operatorname{lcm}(|g|, |h|) = \operatorname{lcm}(m,n) < mn$$

in view of (6). ~~Hence~~ This contradicts $|(g,h)| = mn$. Hence $d > 1$ is not possible. Thus $\gcd(m,n) = 1$, which proves ($\Rightarrow$).

($\Leftarrow$) Let $\gcd(m,n) = 1$. Let $G = \langle g \rangle$, $H = \langle h \rangle$, with $|g| = m$ & $|h| = n$. Then by Theorem 8.1, we have $|(g,h)| = \operatorname{lcm}(m,n)$ $= mn$ because $\gcd(m,n) = 1$. Thus (g,h) is a generator of $G \oplus H$, ie $G \oplus H = \langle (g,h) \rangle$. Hence $G \oplus H$ is cyclic, which proves ($\Leftarrow$) and hence Theorem 2.

Since every finite cyclic group G is isomorphic to $\mathbb{Z}_m$ for some m, we have the following

Corollary: $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if $(m,n) = 1$.