MAS 4301, Abstract Algebra I.

Notes of Krishna Alladi's Lecture on Wed, Apr 1, 2020

Chapter 8: External Direct Products Cont'd.

We begin by noting that Theorem 8.2 (proved in the previous lecture) can be extended to an external direct product of m groups as follows:

Theorem 8.2' (This is Cor 1 on p.160 of the textbook)
Let $G_1, G_2, \cdots, G_m$ be a collection of finite cyclic groups. Let $|G_i| = n_i$, for $i = 1, 2, \cdots, m$. Then $G_1 \oplus G_2 \oplus \cdots \oplus G_m$ is cyclic if and only if

$$\gcd(n_i, n_j) = 1, \quad \forall\, i, j \text{ satisfying } i \neq j \qquad (1)$$

The integers n_i satisfying (1) are said to be pairwise relatively prime.

Just we had a Corollary for Thm 8.2 (see previous lecture), we now have

Corollary': (This is Corollary 2 on p.160 of the textbook)
Let $n_1, n_2, \cdots, n_m$ be positive integers. Then

$$\mathbb{Z}_{n_1 n_2 \cdots n_m} = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m}$$

if and only if the n_i are pairwise relatively prime, ie (1) holds.

We now illustrate Corollary' in the case of two groups G_1 and G_2, $G_1 = \mathbb{Z}_m$ and $G_2 = \mathbb{Z}_n$ (where we have replaced their orders n_1, n_2 by m and n). We assume $(m, n) = 1$, and construct an isomorphism from $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Consider a residue class $[x]_{mn}$ in $\mathbb{Z}_{mn}$ and denote this by x, with $0 \leq x \leq mn - 1$. Each such x when divided by m yields a remainder x_m with $0 \leq x_m \leq m-1$, and when divided by n yields a remainder x_n, with $0 \leq x_n \leq n-1$. Now $x_m \in \mathbb{Z}_m$ and $x_n \in \mathbb{Z}_n$ (by abuse of notation). Thus $(x_m, x_n) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Now consider the map

$$\varphi_s : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n \qquad (2)$$

$$x \longrightarrow (x_m, x_n)$$

where the use of the subscript s in φ_s will become clear soon.

The map φ_s is a homomorphism because the properties of congruences imply that

if $x \to (x_m, x_n)$ & $y \to (y_m, y_n)$, then $x+y \to (x_m+y_m, x_n+y_n)$

But this map is one-to-one because $\varphi_s(x) = \varphi_s(x')$ yields

$$x \equiv x' \pmod m \quad \& \quad x \equiv x' \pmod n$$

$$\Leftrightarrow \quad m \mid x-x' \quad \& \quad n \mid x-x'$$

$$\Rightarrow \quad mn \mid x-x' \quad (\text{because } (m,n)=1).$$

Thus

$$[x]_{mn} = [x']_{mn}$$

which establishes that φ_s is one-to-one. But $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ are sets of equal size. So the one-to-one map will also be onto. This means φ_s is a bijection and is therefore an isomorphism.

We will refer to φ_s as the standard isomorphism and for this reason we have used the subscript s.

Example: We illustrate the standard isomorphism between $\mathbb{Z}_6$ & $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. The elements of $\mathbb{Z}_6$ by abuse of notation are $0, 1, 2, 3, 4, 5$. We will reduce these 6 integers mod 2 and mod 3 to get

φ_s: $\mathbb{Z}_6$	$\to$	$\mathbb{Z}_2 \oplus \mathbb{Z}_3$
0	$\to$	(0,0)
1	$\to$	(1,1)
2	$\to$	(0,2)
3	$\to$	(1,0)
4	$\to$	(0,1)
5	$\to$	(1,2)

Note that $\mathbb{Z}_6 = \langle [1]_6 \rangle = \langle 1 \rangle$

and $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle [1]_2, [1]_3 \rangle = \langle (1,1) \rangle$

because starting with (1,1) and adding it to itself in succession we get

$\langle (1,1) \rangle = \{(1,1), (2,2)=(0,2), (3,3)=(1,0), (4,4)=(0,1), (5,5)=(1,2), (6,6)=(0,0)\}$

More generally if $n_1, n_2, \cdots, n_m$ are pairwise relatively prime, then the <u>standard isomorphism</u>

$$\left.\begin{aligned} \varphi_s &: \mathbb{Z}_{n_1 n_2 \cdots n_m} \to \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m} \\ \text{is given by} \quad \varphi_s &: x \to (x_{n_1}, x_{n_2}, \cdots, x_{n_m}) \end{aligned}\right\} \quad (3)$$

where $[x]_{n_1 n_2 \cdots n_m}$ is a residue class mod $n_1 n_2 \cdots n_m$, denoted by x, and

$$x \equiv x_{n_i} \pmod{n_i}, \text{ for } i = 1, 2, \cdots m. \quad (4)$$

<u>Other isomorphisms</u>: Since $\mathbb{Z}_{n_1 n_2 \cdots n_m}$ is cyclic, there are several isomorphisms (automorphisms) ψ that can be constructed

$$\psi: \mathbb{Z}_{n_1 n_2 \cdots n_m} \to \mathbb{Z}_{n_1 n_2 \cdots n_m}$$

by picking any generator of $\mathbb{Z}_{n_1 n_2 \cdots n_m}$ and mapping it to another generator of $\mathbb{Z}_{n_1 n_2 \cdots n_m}$, and making the mapping to be operation preserving. Then with such a ψ, we can construct isomorphisms from $\mathbb{Z}_{n_1 n_2 \cdots n_m}$ to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m}$ (in the case where n_i are pairwise relatively prime by considering the composition map $\varphi_s \circ \psi$. That is

$$\varphi_s \circ \psi : \mathbb{Z}_{n_1 n_2 \cdots n_m} \to \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m} \quad (5)$$

will be different from the standard isomorphism. We call $\varphi_s \circ \psi$ a <u>non-standard</u> isomorphism. We illustrate a non-standard isomorphism $\mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$ by using the other generator 5 of $\mathbb{Z}_6$:

$\psi: \mathbb{Z}_6 = \langle 1 \rangle \to \mathbb{Z}_6 = \langle 5 \rangle$

$0 \to 0$
$1 \to 5$
$2 \to 4 \quad (\equiv 5+5 \pmod 6)$
$3 \to 3$
$4 \to 2$
$5 \to 1$

$\varphi_s \circ \psi: \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$

$0 \to (0,0)$
$1 \to (1,2)$
$2 \to (0,1)$
$4 \to (0,2)$
$5 \to (1,1)$

Remark: If the integers $n_1, n_2, \cdots, n_m$ are pairwise relatively prime, and if $d \mid n_1 n_2 \cdots n_m$, then it is easy to determine the number of elements of $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_m}$ which have order d. This ~~bec~~is because, Corollary 1 tells us that this number is the same as the number of elements of order d in the cyclic group $\mathbb{Z}_{n_1 n_2 \cdots n_m}$ which is $\varphi(d)$, where φ is Euler's function. So the problem is more interesting in the case where the n_i are not pairwise relatively prime. But then we use Theorem 8.1 from the previous lecture.

Problem 10, p.168: How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have?

Solution: An element $(\alpha, \beta) \in \mathbb{Z}_3 \oplus \mathbb{Z}_9$ has order 9 if and only if $\operatorname{lcm}[|\alpha|, |\beta|] = 9$ (using Thm 8.1). The values of $|\alpha|$ are 1 or 3. So we are forced to have $|\beta| = 9$. The number of elements $\beta \in \mathbb{Z}_9$ of order 9 is $\varphi(9) = 6$, where φ is the Euler function. With regard to α,

$|\alpha| = 1 \Rightarrow \alpha = 0$, the identity in $\mathbb{Z}_3$

$|\alpha| = 3 \Rightarrow \alpha = 1, 2$, the two generators of $\mathbb{Z}_3$.

Thus there are 3 choices of α. So the number of choices of (α, β) with $\operatorname{lcm}[|\alpha|, |\beta|] = 9$ is $3 \times 6 = 18$. Thus there are 18 elements of order 9 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$.

Problem 3, p.168: Let G and H be groups with identities e_G and e_H respectively. Prove that G is isomorphic to $G \oplus \{e_H\}$ and H is isomorphic to $\{e_G\} \oplus H$.

Proof: The map $\phi: G \to G \oplus \{e_H\}$ given by $\phi: g \to (g, e_H)$ for each $g \in G$ is operation preserving and a bijection. Hence it is an isomorphism. Similarly the map $\psi: H \to \{e_G\} \oplus H$ given by $\psi: h \to (e_G, h)$ is an isomorphism.

Remark: Note that $G \oplus \{e_H\}$ is a subgroup of $G \oplus H$ and $\{e_G\} \oplus H$ is a subgroup of $G \oplus H$. This together with the assertion of Problem 3 is useful as the next two results show.

Problem 4, p.168: Let G and H be groups. Prove that $G \oplus H$ is Abelian if and only if G and H are both Abelian.

Proof:

($\Leftarrow$) Let G and H be Abelian. Then by the definition of $G \oplus H$, we see that $G \oplus H$ is Abelian. This proves ($\Leftarrow$)

($\Rightarrow$) Suppose $G \oplus H$ is Abelian. We know all subgroups of an Abelian group are Abelian. Thus $G \oplus \{e_H\}$ and $\{e_G\} \oplus H$ are Abelian since they are subgroups of $G \oplus H$. But then $G \simeq G \oplus \{e_H\}$ and $H \simeq \{e_G\} \oplus H$. Therefore G and H are Abelian. This proves ($\Rightarrow$).

We know that if G and H are cyclic groups, both finite, then $G \oplus H$ is cyclic if and only if $\gcd(|G|, |H|) = 1$. In the other direction we have

Problem 17, p. 168: Let G and H be groups such that $G \oplus H$ is cyclic. Prove that G and H are themselves cyclic.

Proof: We know that every subgroup of a cyclic group is cyclic. Thus $G \oplus \{e_H\}$ and $\{e_G\} \oplus H$ are cyclic since they are both subgroups of the cyclic group $G \oplus H$. But then $G \simeq G \oplus \{e_H\}$ and $H \simeq \{e_G\} \oplus H$. Hence G and H are cyclic groups as well.

Problem 6, p168: Prove that $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ is <u>not</u> isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_2$.

Proof: In $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, the element $(1,0)$ has order 8. (easy to check). The order of each element of $\mathbb{Z}_4$ is 1, 2 or 4. Thus by Theorem 8.1, the possible orders of elements of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ are 1, 2, 4. Hence $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has no element of order 8. Thus $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ cannot be isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ (both groups are of same size).