Finitely Generated Abelian Groups

Def. The **cartesian product** of sets $S_1, \dots, S_n$ is the set of all ordered n-tuples $(a_1, \dots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \dots, n$. We write:

$$S_1 \times S_2 \times \dots \times S_n \text{ or } \prod_{i=1}^{n} S_i$$

Theorem: Let $G_1, G_2, \dots, G_n$ be groups. For $(a_1, a_2, \dots, a_n)$ and $(b_1, b_2, \dots, b_n)$ in $\prod_{i=1}^{n} G_i$

define $(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$.

Then $\prod_{i=1}^{n} G_i$ is a group, the **direct product of the groups G_i**, under this multiplication.

Proof: The $\prod_{i=1}^{n} G_i$ is closed under this multiplication and the multiplication is associative because each component is.

$(e_1, e_2, \dots, e_n)$ is the identity element of $\prod_{i=1}^{n} G_i$, where e_i is the identity element of G_i.

$({a_1}^{-1}, {a_2}^{-1}, \dots, {a_n}^{-1})$ is the inverse of $(a_1, a_2, \dots, a_n)$.

When all of the G_i's are abelian groups, additive notation is sometimes used and $\prod_{i=1}^{n} G_i$ is referred to as the direct sum of the groups G_i and is written $G_1 \oplus G_2 \oplus \dots \oplus G_n$. The direct product (or sum) of abelian groups is also abelian.

Notice that if $|G_i| = r_i$ for $i = 1, \dots, n$ then $\left|\prod_{i=1}^{n} G_i\right| = (r_1)(r_2) \dots (r_n)$.

Ex. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_2$ which has $(3)(2) = 6$ elements:

$(0,0), (0,1), (1,0), (1,1), (2,0)$ and $(2,1)$.

Notice that $\mathbb{Z}_3 \times \mathbb{Z}_2$ is a cyclic group because $(1,1)$ generates the group:

$$1(1,1) = (1,1)$$

$$2(1,1) = (1,1) + (1,1) = (2,0)$$

$$3(1,1) = (1,1) + (1,1) + (1,1) = (0,1)$$

$$4(1,1) = (1,0)$$

$$5(1,1) = (2,1)$$

$$6(1,1) = (0,0).$$

Up to an isomorphism there is only one cyclic group of order n, $\mathbb{Z}_n$. So $\mathbb{Z}_3 \times \mathbb{Z}_2$ is isomorphic to $\mathbb{Z}_6$. This isomorphism, ϕ, can be generated by $\phi(1,1) = 1$ (since $(1,1)$ generates $\mathbb{Z}_3 \times \mathbb{Z}_2$ and 1 generates $\mathbb{Z}_6$).

Ex. Show $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ is not isomorphic to the cyclic group $\mathbb{Z}_{16}$.

It is true that $|G| = 16 = |\mathbb{Z}_{16}|$, but for G to be cyclic we would need to find an element of $\mathbb{Z}_4 \times \mathbb{Z}_4$ which has order 16.

But for any $a \in \mathbb{Z}_4$, $a + a + a + a = 0$ in $\mathbb{Z}_4$.

So any element of $\mathbb{Z}_4 \times \mathbb{Z}_4$, (a, b) has at most order 4.

Thus $\mathbb{Z}_4 \times \mathbb{Z}_4$ is not a cyclic group. In particular, $\mathbb{Z}_4 \times \mathbb{Z}_4$ is **not** isomorphic to $\mathbb{Z}_{16}$.

Theorem: The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to $\mathbb{Z}_{mn}$ if, and only if, m and n are relatively prime (i.e. $GCD(m,n) = 1$).

Proof: If m and n are relatively prime the order of $(1,1)$ is mn since the first component is 0 whenever it is multiplied by a multiple of m and the second is 0 when multiplied by a multiple of n.

If $GCD(m,n) = 1$, then the smallest multiple that make both components 0 is mn.

Since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, (1, 1) generates $\mathbb{Z}_m \times \mathbb{Z}_n$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

To show $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic implies $GCD(m,n) = 1$ we show that if $GCD(m,n) \neq 1$ then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Suppose $GCD(m,n) = d > 1$ then $\frac{mn}{d}$ is divisible by m and n, thus $\frac{mn}{d}(r,s) = (r,s) + (r,s) + \cdots + (r,s) = (0,0)$ for any element $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$. So the order of (r,s) is less than mn.

Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ does not have an element that generates the entire group and $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.

Corollary: The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_n}$ if, and only if, the natural numbers $m_i, i = 1, \dots, n$ are such that the GCD of any two numbers is 1.

Ex. Suppose $n = (p_1)^{m_1}(p_2)^{m_2} \dots (p_r)^{m_r}$ where $p_i,\ i = 1, \dots, r$ are distinct prime numbers and $m_i, i = 1, \dots, r,$ are positive integers then the previous corollary shows:

$\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{(p_1)^{m_1}} \times \mathbb{Z}_{(p_2)^{m_2}} \times \dots \times \mathbb{Z}_{(p_n)^{m_n}}$.

In particular if $n = 360 = 2^3 \times 3^2 \times 5,$

then $\mathbb{Z}_{360}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

Def. Let $r_1, r_2, \dots, r_n$ be positive integers. The **least common multiple** (**LCM**) is the smallest positive integer that is a multiple of each $r_i, i = 1, \dots, n$.

To find the *LCM*, prime factor each number and take the highest power of each prime factor present in any of the numbers and multiply them.

Ex. Find $LCM(5, 12, 18)$.

$$5 = 5^1,\ \ 12 = 2^2 \times 3,\ \ 18 = 2 \times 3^2$$

$$LCM = 2^2 \times 3^2 \times 5 = 180.$$

Notice that the *LCM* is the generator of the cyclic group of all common multiples of $r_1, \dots, r_n$.

Ex. Find the cyclic group of all common multiples of $5, 12,$ and 18 (i.e. $5, 12,$ and 18 divide all elements of this group).

$180\mathbb{Z}$, since $LCM(5, 12, 18) = 180$.

Theorem: Let $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$.

If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$ is equal to the *LCM* of the $r_i's$.

Proof: For $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$, k must be a multiple of r_i for $i = 1, \ldots, n$.

The smallest power for that to be true is $LCM(r_1, \ldots, r_n)$.

Ex. Find the order of $(6, 10, 16)$ in $\mathbb{Z}_{16} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

The order of 6 in $\mathbb{Z}_{16}$ is $\frac{16}{GCD(6,16)} = \frac{16}{2} = 8$

The order of 10 in $\mathbb{Z}_{60}$ is $\frac{60}{GCD(10,60)} = \frac{60}{10} = 6$

The order of 16 in $\mathbb{Z}_{24}$ is $\frac{24}{GCD(16,24)} = \frac{24}{8} = 3$.

So the order of $(6, 10, 16)$ in $\mathbb{Z}_{16} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ is the $LCM(8, 6, 3)$.

$$8 = 2^3, \quad 6 = 2 \times 3, \quad 3 = 3$$

$$LCM(8, 6, 3) = 2^3 \times 3 = 24.$$

So the order of $(6, 10, 16)$ in $\mathbb{Z}_{16} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ is 24.

Ex. What is the largest order among orders of all cyclic subgroups of $\mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$? Find an element that generates a cyclic subgroup of that order.

Let $(a, b, c) \in \mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.

The order of (a, b, c) is the LCM of the orders of in a, b, c in $\mathbb{Z}_9, \mathbb{Z}_{12}$, and $\mathbb{Z}_{15}$ respectively.

The largest possible order for (a, b, c) is $LCM(9, 12, 15)$.

$$9 = 3^2, \qquad 12 = 2^2 \times 3, \qquad 15 = 3 \times 5$$

So $LCM(9, 12, 15) = 2^2 \times 3^2 \times 5 = 180$.

So the order of the largest cyclic subgroup of $\mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is 180.

To find an element of that order, just find

an element in $\mathbb{Z}_9$ of order $3^2 = 9$ $\quad e.g.\ 1$

an element in $\mathbb{Z}_{12}$ of order $2^2 = 4$ $\quad e.g.\ 3$

an element in $\mathbb{Z}_{15}$ of order 5 $\quad e.g.\ 3.$

So $(1, 3, 3) \in \mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ has order 180 and generates a cyclic group of that order.

Notice that $\mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is not isomorphic to $\mathbb{Z}_{(9)(12)(15)} = \mathbb{Z}_{(1620)}$

because there is no element in $\mathbb{Z}_9 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$ of order 1620.

Fundamental Theorem of Finitely Generated Abelian Groups:

Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form:

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \dots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \dots \times \mathbb{Z}$$

where p_i are primes, not necessarily distinct, and the r_i are positive integers.

Ex. Find all abelian groups, up to isomorphism, of order 540.

$540 = 2^2 \times 3^3 \times 5.$

By the previous theorem we get:

$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$G_2 = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$G_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

$G_5 = \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$G_6 = \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5.$