Class 14

March 1, 2024

Direct Products of Groups

We have seen many examples of small groups. Now, we will build bigger groups using smaller groups. One such method is the direct product (often called the product).

Def

Let $(G, *_G)$ and $(H, *_H)$ be groups. Then

$$G \times H = \{(g, h) \,|\, g \in G, h \in H\}$$

under the binary operation $*$

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

forms a group.

Pf

Closure: First, let's show closure. Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

and as G, H are groups, then they are closed under their respective binary operations, thus

$$g_1 *_G g_2 \in G, h_1 *_H h_2 \in H$$

thus

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2) \in G \times H$$

Identity: Now to show identity: Let e_G and e_H be the identity elements in G and H respectively. Let $(g, h) \in G \times H$. Then

$$(e_G, e_H) * (g, h) = (e_G *_G g, e_H *_H h) = (g, h)$$

So (e_G, e_H) is the identity in $G \times H$.

Inverses: Let $(g, h) \in G \times H$. Then $\left(g^{-1}, h^{-1}\right) \in G \times H$ as G and H are groups and each element will have an inverse in the corresponding group. Thus

$$(g, h) * \left(g^{-1}, h^{-1}\right) = \left(g *_G g^{-1}, h *_H h^{-1}\right) = (e_G, e_H)$$

Thus $(g, h)^{-1} = \left(g^{-1}, h^{-1}\right)$.

Associativity: Let $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Then

$$((g_1, h_1) * (g_2, h_2)) * (g_3, h_3) = ((g_1 *_G g_2, h_1 *_H h_2)) * (g_3, h_3)$$

$$= ((g_1 *_G g_2) *_G g_3, (h_1 *_H h_2) *_H h_3) = (g_1 *_G (g_2 *_G g_3), h_1 *_H (h_2 *_H h_3))$$

$$= (g_1, h_1) * (g_2 *_G g_3, h_2 *_H h_3) = (g_1, h_1) * ((g_2, h_2) * (g_3, h_3))$$

As we have shown all of the required properties, then $G \times H$ is a group.

Example 1

Let $G = (\mathbb{Z}, +)$, $H = (\mathbb{Z}, +)$. Then

$$G \times H = \{(a, b) \,|a, b \in \mathbb{Z}\} = \mathbb{Z}^2$$

We add these ordered pairs element-wise. We also may use $+$ rather than $*$ for the binary operation as this is unambiguous. For example:

$$(1, 3) + (2, 4) = (1 + 2, 3 + 4) = (3, 7)$$

Example 2

Let $G = \mathbb{Z}_2$, $H = D_3$. Then

$$G \times H = \left\{(0, e), (0, r), \left(0, r^2\right), (0, f), (0, fr), \left(0, fr^2\right), (1, e), (1, r), \left(1, r^2\right), (1, f), (1, fr), \left(1, fr^2\right)\right\}$$

We can combine elements as is done in the example below:

$$(0, f) * (1, fr) = (0 + 1, f * fr) = (1, r)$$

$$\left(1, r^2\right) * \left(1, r^2\right) = \left(1 + 1, r^2 * r^2\right) = (0, r)$$

Example 3

Let $G = \mathbb{Z}_2$, $H = \mathbb{Z}_3$

$$G \times H = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$$

Here, we need to be careful when combining elements of $G \times H$. We need to respect the modular arithmetic for each coordinate. For example,

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

as the first coordinate is modulo 2 and the second coordinate is modulo 3. Similarly,

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

Comment

Sometimes we may wish to take the product of multiple groups. We often use the shorthand below:

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

When we take this product, we will use the convention below for a generic element of $\times_{i=1}^{n} G_i$.

$$(g_1, g_2, \ldots, g_n) \in \times_{i=1}^{n} G_i$$

This is to avoid nesting a large number of parentheses.

Example 4

Suppose $G_i = \mathbb{Z}_i$. Consider:

$$G = \times_{i=2}^{5} \mathbb{Z}_i = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

so if we add

$$(1, 2, 3, 4) + (1, 2, 3, 4) = (1 + 1, 2 + 2, 3 + 3, 4 + 4) = (0, 1, 2, 3)$$

as the first coordinate is mod 2, the second is mod 3, and so on.

Some properties

1) G, H are abelian groups if and only if $G \times H$ is abelian.

2) If G, H are cyclic groups, then $G \times H$ is cyclic if and only if $|G|, |H|$ are relatively prime.

Proofs of properties

1) Suppose G, H are abelian. Then for $(g_1, h_1), (g_2, h_2) \in G \times H$

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2) = (g_2 *_G g_1, h_2 *_H h_1) = (g_2, h_2) * (g_1, h_1)$$

Now suppose WLOG that H is non-abelian. Then there exists $h_1, h_2 \in H$ such that $h_1 *_H h_2 \neq h_2 *_H h_1$. So for $(g_1, h_1), (g_2, h_2) \in G \times H$:

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

$$(g_2, h_2) * (g_1, h_1) = (g_2 *_G g_1, h_2 *_H h_1)$$

but as $h_1 *_H h_2 \neq h_2 *_H h_1$, then $(g_1 *_G g_2, h_1 *_H h_2) \neq (g_2 *_G g_1, h_2 *_H h_1)$, so $(g_1, h_1) * (g_2, h_2) \neq (g_2, h_2) * (g_1, h_1)$.

2) Suppose $|G| = n, |H| = m$ are not relatively prime. Then the least common multiple of $n, m < nm$. As G, H are cyclic, then for any $g \in G$,

$$g^n = e_G$$

and for any $h \in H$,

$$h^m = e_H$$

so if we take any $(g, h) \in G \times H$, then

$$(g, h)^{\mathrm{LCM}(n,m)} = \left(g^{\mathrm{LCM}(n,m)}, h^{\mathrm{LCM}(n,m)}\right) = (e_G, e_H)$$

but as $\mathrm{LCM}(n, m) < nm$, then it is not possible for any element of $G \times H$ to generate all of the elements of $G \times H$ (as this would require us to visit all of the elements in $G \times H$ exactly once before visiting the identity). Now, suppose $|G| = n, |H| = m$ are relatively prime. Then if $G = \langle g \rangle$, $H = \langle h \rangle$, then

$$g^k = e_G$$

only when $n|k$ and similarly,

$$h^k = e_H$$

only when $m|k$. If we take the element $(g, h) \in G \times H$, then for any number k,

$$(g, h)^k = \left(g^k, h^k\right) = (e_G, e_H)$$

only when $n|k$ and $m|k$. But as n, m are relatively prime, this implies $nm|k$. As $|G \times H| = nm$, then $G \times H$ must be cyclic as every element in $G \times H$ will be visited before the identity.