Products

Definition: Let G and H be groups. The *product group* $G \times H$ is the cartesian product of G and H with group operation $(g, h)(g', h') = (gg', hh')$.

$$\underset{G}{g},\ \underset{H}{h},\ \underset{G}{g'},\ \underset{H}{h'}$$

Proposition: $G \times H$ is a group.

Proof: 1) $\big((g,h)(g',h')\big)(g'',h'') = (g,h)\big((g',h')(g'',h'')\big)$

$= (gg', hh')(g'', h'')$

$= ((gg')g'', (hh')h'')$

$= (g(g'g''), h(h'h'')) = (g,h)(g'g'', h'h'')$

$= (g,h)\left[(g',h')(g'',h'')\right]$

2) (e,e) is the identity.

$(e_G, e_H)(g,h) = (e_G g, e_H h) = (g,h)$

$(g,h)(e_G, e_H) = (ge_G, he_H) = (g,h)$

3) $(g,h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$

So $G \times H$ is a group

Products: Examples

- The space $\mathbb{R}^n$ of n-vectors is a group. It is the product

$$\overbrace{\mathbb{R} \times \cdots \times \mathbb{R}}^{n}$$

$\mathbb{R}$ additive group

$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$

$[a_1, \ldots, a_n] + [b_1, \ldots, b_n]$

$= [a_1 + b_1, \ldots, a_n + b_n]$

identity $= [0, 0, 0, \ldots 0]$

inverse of $[a_1, \ldots, a_n] = [-a_1, \ldots, -a_n]$.

- The group $\mathbb{Z}_2^n$ is the space of $0-1$ vectors with componentwise addition.

$\mathbb{Z}_2^n = \overbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}^{n \text{ times}}$

	0	1
0	0	1
1	1	0

exclusive or

$a = (0, 1, 1, 0, 0, \ldots, 1)$ $b = (1, 1, 0, \ldots, 0)$

$a + b = (1, 0, 1, \ldots)$

$(0111) + (1010) = (1101)$

- The group $\mathbb{R} \times \mathbb{Z}$ consists of pairs (r, n) with $r \in \mathbb{R}$ and $n \in \mathbb{Z}$, and addition on components.

$\mathbb{R} \times \mathbb{Z} = \{(r, n) \mid r \in \mathbb{R}, n \in \mathbb{Z}\}$

$(\pi, -5) + (14, -2)$

$= (14 + \pi, -7)$

-3 -2 -1 0 1 2 3

Products and Orders

Theorem: Let G and H be groups, and let $(g,h) \in G \times H$. If g has finite order r and h has finite order s, then (g,h) has order $lcm(r,s)$.

$\mathbb{Z}_{\cancel{4}6} \times \mathbb{Z}_4$

$2 \in \mathbb{Z}_6 \quad \text{order}(2) = \frac{6}{\gcd(2,6)} = \frac{6}{2} = 3$

$3 \in \mathbb{Z}_4 \quad \text{order}(3) = \frac{4}{\gcd(3,4)} = 4$

$\text{lcm}(3,4) = 12$

$(2,3)^1 \qquad (4,6) = (4,2)^2 \qquad (0,1)^3$

$1 \cdot g \qquad 2 \cdot g$

$(2,0)^4 \qquad (4,3)^5 \qquad (6,6)^6 = (0,2)$

$(2,1)^7 \qquad (4,0)^8 \qquad (0,3)^9$

$(2,2)^{10} \qquad (4,1)^{11} \qquad (6,0)^{12}$

Proof: $(g,h)^m = \underbrace{(g,h)(g,h)\cdots(g,h)}_{m \text{ times}} = (g^m, h^m)$

Suppose $(g,h)^m = (e,e)$. Then $g^m = e$ and $h^m = e$.
order$(g) | m$ and order$(h) | m$, so m is a common multiple of order$(g) = r$ and order$(h) = s$. Order is smallest common multiple.

$(g,h)^{lcm(r,s)} = (g^{\overbrace{lcm(r,s)}^{\text{multiple of } r}}, h^{\overbrace{lcm(r,s)}^{\text{multiple of } s}}) = (e, e)$

Corollary: Suppose, for $i = 1, \ldots, n$, that G_i is a group. If

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

and g_i has order r_i, then the order of g is the least common multiple of the r_i.

$$\prod_{i=1}^{n} G_i \simeq G_1 \times G_2 \times \cdots \times G_n$$

$$(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$$

$$(g_1, \ldots, g_n)^m = (e, \ldots, e).$$

$\text{order}(g_i) \mid m$ for all i so m has to be a common multiple. Smallest possible common multiple is $L = \text{lcm}(\text{order}(g_1), \text{order}(g_2), \ldots \text{order}(g_n))$

$$(g_1, \ldots, g_n)^L = (g_1^L, \ldots g_n^L) = (e, \ldots, e).$$

Since L is a multiple of $\text{order}(g_i)$

$$g_i^L = g_i^{\text{order}(g_i)?} = e.$$

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

$(1,1,1) \in G$ orders are 2, 3, and 5

$\text{lcm}(2,3,5) = 30$

$(1,1,1)$ has order 30.

$G = \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_{10}$

$(1,1,1)$

$\text{lcm}(4,6,10) = 60$

$\text{order}(1,1,1) = 60.$

Theorem: The groups $\mathbb{Z}_n \times \mathbb{Z}_m$ and $\mathbb{Z}_{nm}$ are isomorphic if and only if $gcd(m,n) = 1$.

isomorphic.

E.g. $\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$ $\qquad gcd(3,5) = 1$

$\mathbb{Z}_4 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{28}$

$\mathbb{Z}_{60} \simeq \mathbb{Z}_{4} \times \mathbb{Z}_{15}$

Proof: ① every cycle group of order n is isomorphic to $\mathbb{Z}_n$.

it's enough to show that

$\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic if $gcd(n,m) = 1$.

Take $(1,1) \in \mathbb{Z}_n \times \mathbb{Z}_m$

what is its order?

order(1) in $\mathbb{Z}_n$ is n

order(1) in $\mathbb{Z}_m$ is m.

order$(1,1)$ = lcm(n,m).

Since $gcd(n,m)=1$, $\quad lcm(n,m) = nm$.

$gcd(n,m)\, lcm(n,m) = nm$.

$$lcm(n,m) = \frac{mn}{gcd(n,m)}.$$

order$(1,1) = nm$.

$\mathbb{Z}_n \times \mathbb{Z}_m$ has nm elements and $(1,1)$ of order nm.

$\langle (1,1) \rangle \leq \mathbb{Z}_n \times \mathbb{Z}_m$ and both have nm elts.

so $\langle (1,1) \rangle = \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

Corollary: Every cyclic group is a product of cyclic groups of prime power order. More precisely, given an integer n with prime factorization

$$\underline{n = p_1^{e_1} \cdots p_k^{e_k}}$$

where the p_i are distinct primes, then

$$\underline{\mathbb{Z}_n} = \underline{\mathbb{Z}_{p_1^{e_1}}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

$60 = 2^2 \cdot 3 \cdot 5$

$\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5.$

$\mathbb{Z}_{60} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$12 = 2^2 \cdot 3$

$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$

Pf: $(1, 1, 1, \ldots, 1) \in \mathbb{Z}_{p_1^{e_1}} \times \cdots \mathbb{Z}_{p_k^{e_k}}$

order $= \operatorname{lcm}(p_1^{e_1}, \ldots, p_k^{e_k}) = p_1^{e_1} \cdots p_k^{e_k}$

$\langle (1, \ldots, 1) \rangle$ has $p_1^{e_1} \cdots p_k^{e_k}$ elts.

$\subseteq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ which also has $p_1^{e_1} \cdots p_k^{e_k}$ elts

So $\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ is cyclic with n elts so it is $\mathbb{Z}_n$ up to isomorphism.

$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$

$(1,1) \in \mathbb{Z}_4 \times \mathbb{Z}_3$

$$
\begin{aligned}
f : \mathbb{Z}_4 \times \mathbb{Z}_3 &\longrightarrow \mathbb{Z}_{12} \\
(1,1) &\longrightarrow 1 \\
(2,2) &\longrightarrow 2 \\
(3,0) &\longrightarrow 3 \\
(0,1) &\longrightarrow 4 \\
(1,2) &\longrightarrow 5 \\
(2,0) &\longrightarrow 6 \\
(3,1) &\longrightarrow 7 \\
(0,2) &\longrightarrow 8 \\
(1,0) &\longrightarrow 9 \\
(2,1) &\longrightarrow 10 \\
(3,2) &\longrightarrow 11 \\
(0,0) &\longrightarrow 12 = 0
\end{aligned}
$$

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

$\shortparallel$

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