Products and Finitely generated groups

Defn Let G, H be two groups. Then the direct product $(G\times H, *)$ is defined ~~by~~ by $(g_1, h_1) * (g_2, h_2) := (g_1 g_2, h_1 h_2)$

- $*$ is clearly a binary operation
- Associativity $(g_1,h_1)*\big((g_2,h_2)*(g_3,h_3)\big) = (g_1,h_1)*(g_2g_3, h_2h_3)$
$= (g_1g_2g_3, h_1h_2h_3)$
$= \big((g_1g_2)g_3, (h_1h_2)h_3\big)$
$= \cdots$ (finish it by yourself)
- (e_G, e_H) is the identity
- $(g,h)^{-1} = (g^{-1}, h^{-1})$.

Exercise: ~~Define~~ Define $G_1 \times \cdots \times G_n$ where G_i are all groups. More generally, given any collection $\{G_i\}_i$, define a direct product $\prod_i G_i$.

Ex. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a group with 4 elements. It's NOT isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Pf Assume $\exists$ an isomorphism $\psi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then the order of elements are preserved by ψ (explain in class/verify by yourself).

minimal l s.t. $x^l = e$

In particular $[1] \in \mathbb{Z}/4\mathbb{Z}$ has order 4 $\Rightarrow \psi([1])$ has order 4. But no element of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4 (they all have order 1 or 2). Thus $\nexists$ a ψ $\blacksquare$

Defn • Given $n, m \in \mathbb{Z}$, the greatest common divisor of n, m denoted by $\gcd(n,m)$ is the largest positive integer dividing n and m.
• If $\gcd(n,m) = 1$, then m, n are said to be relatively prime.

Ex $\gcd(4,9) = 1$, $\gcd(6,9) = 3$, $\gcd(-4,4) = 4$.

Prop Let p be a prime number and $a, b \in \mathbb{Z}$. Then $p \mid (ab) \Rightarrow p \mid a$ or $p \mid d$

Thm [Fundamental theorem of Arithmetic] Every $a \in \mathbb{Z}_{>0}$, can be written as a product of primes $a = p_1 \cdots p_r$ that's unique up to reordering.

Defn Given $a, b \in \mathbb{Z} - \{0\}$, the least common multiple of a, b, denoted $\text{lcm}(a,b)$ is the smalest positive m such that $a \mid m$ and $b \mid n$.

[One can show that if $a \mid d$ and $b \mid d \Rightarrow \text{lcm}(a,b) \mid d$]

Prop Let $x \in G$, $y \in H$ be elements of finite orders n, m, respectively. Then $(x,y) \in G \times H$ has order $\text{lcm}(n,m)$.

Pf Let $d = \text{ord}(x,y)$. Then $(e_G, e_H) = (x,y)^d = (x^d, y^d)$

$$\Rightarrow x^d = e_G, \quad y^d = e_H.$$

By division algorithm, $d = q \cdot n + r$ with $0 \le r < n-1$.

Thus $e_G = x^d = x^{q \cdot n + r} = x^{q \cdot n} \cdot x^r = (x^n)^q \cdot x^r = e_G^q \cdot x^r = x^r$.

If $r > 0$, this contradicts the minimality of n (i.e. $\text{ord}\, x =$ minimum positive p s.t. $x^p = e_G$)

Thus $r = 0 \Rightarrow d = qn \Rightarrow n \mid d$. Similarly $m \mid d$.

Thus $\text{lcm}(n,m) \le d$.

On the other hand $(x,y)^{\text{lcm}(n,m)} = (x^{\text{lcm}(n,m)}, y^{\text{lcm}(n,m)}) = (e_G, e_H)$.

Thus $\text{ord}(x,y) = \text{lcm}(n,m)$ ■

Prop. For $[a] \in \mathbb{Z}/n\mathbb{Z}$, ord $[a] = \dfrac{n}{\gcd(a,n)}$.

Pf Think of prime factorization.

Write $a = \gcd(a,n) \cdot a'$, $n = \gcd(a,n)\, n'$. Then $\underbrace{[a] + \cdots + [a]}_{n' \text{ times}} = [0]$.

Fact: $\text{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b$