Direct Products and Finitely Generated Abelian Groups §11

Def 11.1 The Cartesian product of sets $A_1, \dots, A_n$ is the set of ordered n-tuples $(a_1, \dots, a_n)$ where $a_i \in A_i$ for $i = 1, \dots, n$. It is denoted either

$$A_1 \times \dots \times A_n \quad \text{or} \quad \prod_{i=1}^{n} A_i .$$

If $|A_i| = r_i$ for all i, then $|A_1 \times \dots \times A_n| = r_1 \cdots r_n$

Thm 11.2 Let $G_1, \ldots, G_n$ be groups with operation $*_i$ on G_i. Then $G = \prod_{i=1}^{n} G_i$ with operation $*$

$$(g_1, \ldots, g_n) * (g_1', \ldots, g_n') := (\underbrace{g_1 *_1 g_1'}_{\in G_1}, \ldots\ldots, \underbrace{g_n *_n g_n'}_{\in G_n})$$

is a group.

Proof $*$ is a binary operation ✓ see text

G1 associativity: $(a_1, \ldots, a_n)[(b_1 \ldots b_n)(c_1, \ldots, c_n)] = [(a_1 \ldots a_n)(b_1 \ldots b_n)](c_1 \ldots c_n)$

G2 identity: $(e_1, \ldots, e_n) \in G$ is the identity for $*$ where e_i is identity in G_i

G3 inverse: $(a_1, \ldots, a_n) \in G$ has inverse $(a_1^{-1}, \ldots, a_n^{-1}) \in G$ since $(a_1, \ldots, a_n) * (a_1^{-1}, \ldots, a_n^{-1}) = (a_1 a_1^{-1}, \ldots, a_n a_n^{-1}) = (e_1, \ldots, e_n)$ ☐

Ex 11.3 $\mathbb{Z}_2 \times \mathbb{Z}_3$ has order $6 = |\mathbb{Z}_2 \times \mathbb{Z}_3|$.

$$
\begin{aligned}
(1,1) &= (1,1) \\
2(1,1) &= (1,1) + (1,1) = (0,2) \\
3(1,1) &= (1,1) + (1,1) + (1,1) = (1,0) \\
4(1,1) &= 3(1,1) + (1,1) = (1,0) + (1,1) = (0,1) \\
5(1,1) &= 4(1,1) + (1,1) = (0,1) + (1,1) = (1,2) \\
6(1,1) &= 5(1,1) + (1,1) = (1,2) + (1,1) = (0,0) = e.
\end{aligned}
$$

$(1,1)$ has order 6 in $\mathbb{Z}_2 \times \mathbb{Z}_3$

$\langle (1,1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$

is cyclic

$\Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Ex 11.4 $\mathbb{Z}_3 \times \mathbb{Z}_3$ has order 9 but $\forall\, a, b \in \mathbb{Z}_3$

$(a,b) + (a,b) + (a,b) = (3a, 3b) = (0,0) \Rightarrow$ no elt of order 9 in $\mathbb{Z}_3 \times \mathbb{Z}_3$. So this group is <u>not</u> cyclic

Thm 11.5 The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if m, n are relatively prime.

Proof $\Leftarrow$ If m, n are relatively prime then $|\langle (1,1) \rangle| = mn$ since $k(1,1) = (0,0) \Rightarrow m$ and n both divide k, smallest such $k \in \mathbb{Z}^+$ is $m \cdot n$ if rel. prime $\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\cong \mathbb{Z}_{mn}$.

$\Rightarrow$ If $\gcd(m,n) = d$, then $\frac{mn}{d}(a,b) = (0,0)$ for $a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_n$. Hence, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. $\square$

Corollary 11.6 The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 \cdots m_n}$ if and only if

$$\gcd(m_i, m_j) = 1 \quad \forall\ i \neq j.$$

Def 11.8 Let $r_1, \dots, r_n \in \mathbb{Z}^+$. Their least common multiple $\operatorname{lcm}(r_1, \dots, r_n)$ is the unique positive generator of the cyclic subgroup $\{k \in \mathbb{Z} \mid r_i \text{ divides } k \text{ for } \forall\ i = 1, \dots, n\} \leq (\mathbb{Z}, +)$

* compare this with $\operatorname{lcm}(r_1, \dots, r_n) = r$ smallest $r \in \mathbb{Z}^+$ s.t. r_i divides r $\forall\ i = 1, \dots, n$.

Thm 11.9 Let $(a_1, \ldots, a_n) \in \prod_{i=1}^{n} G_i = G$. If a_i is of finite order r_i in G_i then $\operatorname{ord}((a_1, \ldots, a_n))$ in G is $\operatorname{lcm}(r_1, \ldots, r_n)$.

Proof If $(a_1, \ldots, a_n)^r = (a_1^r, \ldots, a_n^r) = (e_1, \ldots, e_n) = e$ then $\operatorname{ord}(a_i) = r_i$ divides r for all i.

$\operatorname{ord}(a_1, \ldots, a_n)$ is least such $r \in \mathbb{Z}^+ \Rightarrow$

$\operatorname{ord}(a_1, \ldots, a_n) = \operatorname{lcm}(r_1, \ldots, r_n)$

* think back to zoom experiments with orders of perms.

Def An abelian group $(G,+)$ is *finitely generated* if $\exists\ g_1,\dots,g_k \in G$ s.t. $G = \{a_1g_1 + a_2g_2 + \dots + a_kg_k \mid a_i \in \mathbb{Z}\}$

Thm 11.12 Fundamental Thm of Finitely Generated Abelian Groups

Every finitely generated abelian group is isomorphic to

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

where p_i's are not necess. distinct primes and the r_i's are positive integers.