Introduction to Modern Algebra

Part Part II. Permutations, Cosets, and Direct Products

II.11. Direct Products and Finitely Generated Abelian Groups

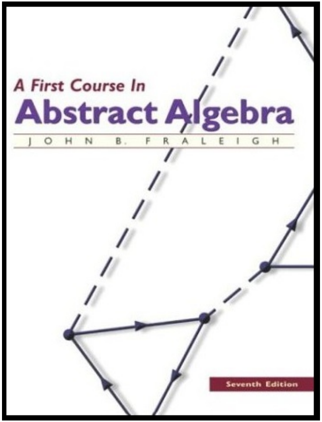

Table of contents

Theorem 11.2

Theorem 11.2. Let $G_1, G_2, \ldots, G_n$ be (multiplicative) groups. For $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in \prod_{i=1}^n G_1$, define the (multiplicative) binary operation $(a_1, a_2, ..., a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^n G_i$ is a group under this binary operation.

Proof. Notice that, by definition, $\prod_{i=1}^n G_1$ is closed under the introduced binary operation. We now verify that $\prod G_i$ satisfies the definition of group. Associativity in $\prod G_i$ holds (G_1) because:

$$\begin{aligned}
& (a_1, a_2, \ldots, a_n)\left((b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)\right) \\
= \; & (a_1, a_2, \ldots, a_n)(b_1 c_1, b_2 c_2, \ldots, b_n c_n) \\
= \; & \left(a_1 (b_1 c_1), a_2 (b_2 c_2), \cdots, a_n (b_n c_n)\right) \\
= \; & \left((a_1 b_1) c_1, (a_2 b_2) c_2, \cdots, (a_n b_n) c_n\right) \text{ since each } G_i \text{ is a group} \\
& \text{and so associativity holds in each } G_i \\
= \; & (a_1 b_1, a_2 b_2, \cdots a_n b_n)(c_1, c_2, \cdots, c_n) \\
= \; & \left((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)\right)(c_1, c_2, \cdots, c_n).
\end{aligned}$$

Theorem 11.2

Theorem 11.2. Let $G_1, G_2, \ldots, G_n$ be (multiplicative) groups. For $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in \prod_{i=1}^n G_1$, define the (multiplicative) binary operation $(a_1, a_2, ..., a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^n G_i$ is a group under this binary operation.

Proof. Notice that, by definition, $\prod_{i=1}^n G_1$ is closed under the introduced binary operation. We now verify that $\prod G_i$ satisfies the definition of group. Associativity in $\prod G_i$ holds $(\mathcal{G}_1)$ because:

$$\begin{aligned}
& (a_1, a_2, \ldots, a_n)\left((b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)\right) \\
= \;& (a_1, a_2, \ldots, a_n)(b_1 c_1, b_2 c_2, \ldots, b_n c_n) \\
= \;& \left(a_1 (b_1 c_1), a_2 (b_2 c_2), \cdots, a_n (b_n c_n)\right) \\
= \;& \left((a_1 b_1) c_1, (a_2 b_2) c_2, \cdots, (a_n b_n) c_n\right) \text{ since each } G_i \text{ is a group} \\
& \text{and so associativity holds in each } G_i \\
= \;& (a_1 b_1, a_2 b_2, \cdots a_n b_n)(c_1, c_2, \cdots, c_n) \\
= \;& \left((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)\right)(c_1, c_2, \cdots, c_n).
\end{aligned}$$

Theorem 11.2 (continued).

Theorem 11.2. Let $G_1, G_2, \ldots, G_n$ be (multiplicative) groups. For $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in \prod_{i=1}^{n} G_1$, define the (multiplicative) binary operation $(a_1, a_2, ..., a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^{n} G_i$ is a group under this binary operation.

Proof (continued). Next, there is an identity in $\prod G_i$, namely $(e_1, e_2, \cdots, e_n)$ where e_i is the identity in G_i:

$$(e_1, e_2, \cdots, e_n)(a_1, a_2, \cdots, a_n) = (e_1 a_1, e_2 a_2, \cdots e_n a_n) = (a_1, a_2, \cdots, a_n)$$

for all $(a_1, a_2, \cdots, a_n) \in \prod G_i$, and so G_2 holds.

Finally, for $(a_1, a_2, \cdots, a_n) \in \prod G_i$, consider $\left(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1}\right) \in \prod G_i$ ($a_i \in G_i$ has inverse $a_i^{-1} \in G_i$ since G_i is a group). Then $(a_1, a_2, \cdots, a_n)\left(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1}\right) = \left(a_1 a_1^{-1}, a_2 a_2^{-1}, \cdots, a_n a_n^{-1}\right) = (e_1, e_2, \cdots, e_n)$, and every element of $\prod G_i$ has an inverse. So G_3 holds and $\prod G_i$ is a group. □

Theorem 11.2 (continued).

Theorem 11.2. Let $G_1, G_2, \ldots, G_n$ be (multiplicative) groups. For $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in \prod_{i=1}^n G_1$, define the (multiplicative) binary operation $(a_1, a_2, ..., a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^n G_i$ is a group under this binary operation.

Proof (continued). Next, there is an identity in $\prod G_i$, namely $(e_1, e_2, \cdots, e_n)$ where e_i is the identity in G_i:
$(e_1, e_2, \cdots, e_n)(a_1, a_2, \cdots, a_n) = (e_1 a_1, e_2 a_2, \cdots e_n a_n) = (a_1, a_2, \cdots, a_n)$
for all $(a_1, a_2, \cdots, a_n) \in \prod G_i$, and so G_2 holds.

Finally, for $(a_1, a_2, \cdots, a_n) \in \prod G_i$, consider $\left(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1}\right) \in \prod G_i$ ($a_i \in G_i$ has inverse $a_i^{-1} \in G_i$ since G_i is a group). Then $(a_1, a_2, \cdots, a_n)\left(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1}\right) = \left(a_1 a_1^{-1}, a_2 a_2^{-1}, \cdots, a_n a_n^{-1}\right) = (e_1, e_2, \cdots, e_n)$, and every element of $\prod G_i$ has an inverse. So G_3 holds and $\prod G_i$ is a group. $\square$

Theorem 11.5.

Theorem. 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime (i.e., $\gcd(m, n) = 1$).

Proof. Consider the cyclic subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $(1, 1)$. By Theorem 6.10 proof Case *II*, the order of $\langle(1, 1\rangle$ is the order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. The order of $(1, 1)$ is k where k is the smallest natural number such that (in additive notation) $k(1, 1) = (0, 0)$ (where $(0, 0)$ is the identity in $\mathbb{Z}_m \times \mathbb{Z}_n$).

Theorem 11.5.

Theorem. 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime (i.e., $\gcd(m, n) = 1$).

Proof. Consider the cyclic subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $(1, 1)$. By Theorem 6.10 proof Case II, the order of $\langle(1, 1\rangle$ is the order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. The order of $(1, 1)$ is k where k is the smallest natural number such that (in additive notation) $k(1, 1) = (0, 0)$ (where $(0, 0)$ is the identity in $\mathbb{Z}_m \times \mathbb{Z}_n$).

Now $k(1, 1) = (k, k) = (0, 0)$ only if k is both a multiple of m and a multiple of n. The smallest such k is the least common multiple of m and n, $k = \mathrm{lcm}(m, n)$. If m and n are relatively prime, then by Exercise 6.47b, $k = mn$. So if m and n are relatively prime (i.e., $\gcd(m, n) = 1$), then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic (with generator $(1, 1)$).

Theorem 11.5.

Theorem. 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime (i.e., $\gcd(m, n) = 1$).

Proof. Consider the cyclic subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by $(1, 1)$. By Theorem 6.10 proof Case II, the order of $\langle(1, 1\rangle$ is the order of $(1, 1)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$. The order of $(1, 1)$ is k where k is the smallest natural number such that (in additive notation) $k(1, 1) = (0, 0)$ (where $(0, 0)$ is the identity in $\mathbb{Z}_m \times \mathbb{Z}_n$).

Now $k(1, 1) = (k, k) = (0, 0)$ only if k is both a multiple of m and a multiple of n. The smallest such k is the least common multiple of m and n, $k = \operatorname{lcm}(m, n)$. If m and n are relatively prime, then by Exercise $6.47b$, $k = mn$. So if m and n are relatively prime (i.e., $\gcd(m, n) = 1$), then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic (with generator $(1, 1)$).

Theorem 11.5 (Continued).

Theorem 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime (i.e., $\gcd(m,n) = 1$).

Proof (continued). Next, suppose m and n are not relatively prime That is, suppose $\gcd(m,n) = d > 1$. Then $\frac{mn}{d}$ is divisible by both m and n. Then for any $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ we have

$$\frac{mn}{d}(r,s) = \left(\frac{mn}{d}r, \frac{mn}{d}s\right) = \left(\frac{n}{d}(mr), \frac{m}{d}(ns)\right) = (0,0).$$

So (r,s) generates a subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ of order at most $\frac{mn}{d} < mn$ and since $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements, (r,s) does not generate $\mathbb{Z}_m \times \mathbb{Z}_n$ and since $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ are arbitrary, no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ generates the group. That is, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. This proves that if $\gcd(m,n) \neq 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. The contrapositive of their statement is that if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then $\gcd(m,n) = 1$. □

Theorem 11.5 (Continued).

Theorem 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime (i.e., $\gcd(m, n) = 1$).

Proof (continued). Next, suppose m and n are not relatively prime That is, suppose $\gcd(m, n) = d > 1$. Then $\frac{mn}{d}$ is divisible by both m and n. Then for any $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ we have

$$\frac{mn}{d}(r, s) = \left(\frac{mn}{d}r, \frac{mn}{d}s\right) = \left(\frac{n}{d}(mr), \frac{m}{d}(ns)\right) = (0, 0).$$

So (r, s) generates a subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ of order at most $\frac{mn}{d} < mn$ and since $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements, (r, s) does not generate $\mathbb{Z}_m \times \mathbb{Z}_n$ and since $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ are arbitrary, no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ generates the group. That is, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. This proves that if $\gcd(m, n) \neq 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. The contrapositive of their statement is that if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then $\gcd(m, n) = 1$. $\square$

Theorem 11.9.

Theorem. 11.9. Let $(a_1, a_2, \ldots, a_n) \in \prod G_i$. If a_i is of finite order r_i, $(a_1, a_2, \ldots, a_n)$ in $\prod G_i$ is the least common multiple of the $\text{lcm}\,(r_1, r_2, \ldots, r_n)$.

Proof. Suppose $(a_1, a_2, \ldots, a_n)^m = (e_1, e_2, \ldots, e_n)$. Then $a_1^m = e_1, a_2^m = e_2, \ldots, a_n^m = e_n$. Then m must be a multiple of $r_1, r_2, \ldots, r_n$. The smallest such m is $\text{lcm}\,(r_1, r_2, \ldots, r_n)$ and so this the order of $(a_1, a_2, \ldots, a_n)$. □

Theorem 11.9.

Theorem. 11.9. Let $(a_1, a_2, \ldots, a_n) \in \prod G_i$. If a_i is of finite order r_i, $(a_1, a_2, \ldots, a_n)$ in $\prod G_i$ is the least common multiple of the lcm $(r_1, r_2, \ldots, r_n)$.

Proof. Suppose $(a_1, a_2, \ldots, a_n)^m = (e_1, e_2, \ldots, e_n)$. Then $a_1^m = e_1, a_2^m = e_2, \ldots, a_n^m = e_n$. Then m must be a multiple of $r_1, r_2, \ldots, r_n$. The smallest such m is lcm $(r_1, r_2, \ldots, r_n)$ and so this the order of $(a_1, a_2, \ldots, a_n)$. □

Theorem 11.15.

Theorem 11.15. The finite indecomposable abelian group are exactly the cyclic groups with order a power of a prime.

Proof. Let G be a finite indecomposable abelian group. Then by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), G is isomorphic to a direct product of cyclic groups of prime power order (and Betti number 0 since G is of finite under). Since G is by hypothesis indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime.

Now suppose G is a cyclic group of order a power of a prime, say (up to isomorphic) $\mathbb{Z}_{p^r}$. By the Fundamental Theorem, if $\mathbb{Z}_{p^r}$ is decomposable then $\mathbb{Z}_{p^r} \cong \mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ where $i = 1, j = 1, i + j = r$. But by Theorem 11.5, $\mathbb{Z}_{p^r}$ is not isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ since p^i and p^j are not relatively prime. So $\mathbb{Z}_{p^r}$ is indecomposable. □

Theorem 11.15.

Theorem 11.15. The finite indecomposable abelian group are exactly the cyclic groups with order a power of a prime.

Proof. Let G be a finite indecomposable abelian group. Then by the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), G is isomorphic to a direct product of cyclic groups of prime power order (and Betti number 0 since G is of finite under). Since G is by hypothesis indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime.

Now suppose G is a cyclic group of order a power of a prime, say (up to isomorphic) $\mathbb{Z}_{p^r}$. By the Fundamental Theorem, if $\mathbb{Z}_{p^r}$ is decomposable then $\mathbb{Z}_{p^r} \cong \mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ where $i = 1, j = 1, i + j = r$. But by Theorem 11.5, $\mathbb{Z}_{p^r}$ is not isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ since p^i and p^j are not relatively prime. So $\mathbb{Z}_{p^r}$ is indecomposable. $\square$

Theorem 11.16.

Theorem 11.16. If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof. By the Fundamental Theorem, G is (isomorphic to the form) $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$. where the primes p_j need to be distinct. Then order of G is $|G| = (p_1)^{r_1} (p_2)^{r_2} \cdots (p_n)^{r_n}$ so m being a division of $|G|$, we must have $m = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_n)^{s_n}$ for some $0 \leq s_i \leq r_i$ for $i = 1, 2, \ldots, n$.

Theorem 11.16.

Theorem 11.16. If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof. By the Fundamental Theorem, G is (isomorphic to the form) $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$. where the primes p_j need to be distinct. Then order of G is $|G| = (p_1)^{r_1}(p_2)^{r_2}\cdots(p_n)^{r_n}$ so m being a division of $|G|$, we must have $m = (p_1)^{s_1}(p_2)^{s_2}\cdots(p_n)^{s_n}$ for some $0 \leq s_i \leq r_i$ for $i = 1, 2, \ldots, n$. By Theorem 6.14, $(p_i)^{r_i - s_i} \in \mathbb{Z}_{(p_i)^{r_i}}$ generates a subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order $\frac{(p_i)}{\gcd((p_i)^{r_i},(p_i)^{r_i-s_i})} = (p_i)^{s_i}$. This subgroup $a = 1$ and $a^s = (p_i)^{r_i - s_i} \times 1 = b = s$ is $\langle (p_i)^{r_i - s_i} \rangle$. So the subgroup of order m is $\langle (p_i)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \cdots \times \langle (p_n)^{r_n - s_n} \rangle$. □

Theorem 11.16.

Theorem 11.16. If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof. By the Fundamental Theorem, G is (isomorphic to the form) $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$. where the primes p_j need to be distinct. Then order of G is $|G| = (p_1)^{r_1} (p_2)^{r_2} \cdots (p_n)^{r_n}$ so m being a division of $|G|$, we must have $m = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_n)^{s_n}$ for some $0 \leq s_i \leq r_i$ for $i = 1, 2, \ldots, n$. By Theorem 6.14, $(p_i)^{r_i - s_i} \in \mathbb{Z}_{(p_i)^{r_i}}$ generates a subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order $\frac{(p_i)}{\gcd((p_i)^{r_i}, (p_i)^{r_i - s_i})} = (p_i)^{s_i}$. This subgroup $a = 1$ and $a^s = (p_i)^{r_i - s_i} \times 1 = b = s$ is $\langle (p_i)^{r_i - s_i} \rangle$. So the subgroup of order m is $\langle (p_i)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \cdots \times \langle (p_n)^{r_n - s_n} \rangle$. $\square$

Theorem 11.17.

Theorem. 11.17. If M is a square free integer (that is, no prime factor of m is of multiplicity greater than 1), then every abelian group of order m is cyclic.

Proof. Let G be an abelian group of square free order m. So $m = p_1 p_2 \cdots p_n$ where the p_i are distinct. By the Fundamental Theorem,

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}.$$

By Corollary 11.6, $G \cong \mathbb{Z}_{p_1 p_2 \cdots p_n}$ (since the p_i, being prime, are pairwise relatively prime) and so G is cyclic. □

Theorem 11.17.

Theorem. 11.17. If M is a square free integer (that is, no prime factor of m is of multiplicity greater than 1), then every abelian group of order m is cyclic.

Proof. Let G be an abelian group of square free order m. So $m = p_1 p_2 \cdots p_n$ where the p_i are distinct. By the Fundamental Theorem,

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}.$$

By Corollary 11.6, $G \cong \mathbb{Z}_{p_1 p_2 \cdots p_n}$ (since the p_i, being prime, are pairwise relatively prime) and so G is cyclic. $\square$