3.2.4. Show that the permutation group S_n is a semidirect product of $\mathbb{Z}_2$ and the group of even permutations A_n.

3.2.5. Consider the set G of n-by-n matrices with entries in $\{0, \pm 1\}$ that have exactly one nonzero entry in each row and column. These are called signed permutation matrices. Show that G is a group, and that G is a semidirect product of S_n and the group of diagonal matrices with entries in $\{\pm 1\}$. S_n acts on the group of diagonal matrices by permutation of the diagonal entries.

One final example shows that direct products and semidirect products do not exhaust the ways in which a normal subgroup N and the quotient group G/N can be fit together to form a group G:

3.2.6. $\mathbb{Z}_4$ has a subgroup isomorphic to $\mathbb{Z}_2$, namely the subgroup generated by $[2]$. The quotient $\mathbb{Z}_4/Z_2$ is also isomorphic to $\mathbb{Z}_2$. Nevertheless, $\mathbb{Z}_4$ is not a direct or semidirect product of two copies of $\mathbb{Z}_2$.

3.3. Finite Abelian Groups

In this section, we will obtain a definitive structure theorem and classification of finite abelian groups. The theorem states that any finite abelian group is a direct product of cyclic groups each of order a power of a prime; furthermore, the number of the cyclic subgroups appearing in the direct product decomposition, and their orders, are unique.

Two finite abelian groups are isomorphic if, and only if, they have the same decomposition into a direct product of cyclic groups of prime power order.

All the groups in this section will be abelian, and, following a common convention, we will use additive notation for the group operation. In particular, the s^{th} power of an element x will be written as sx, and the order of an element x is the smallest natural number s such that $sx = 0$. All subgroups are normal, and the subgroup generated by a family $A_1, \ldots A_s$ of subgroups is $A_1 + \cdots + A_s = \{a_1 + \cdots + a_s : a_i \in A_i \text{ for all } i\}$.

We have the following elementary results on direct products of abelian groups, which may remind you of a result from linear algebra.

Proposition 3.3.1. *Let G be an abelian group with subgroups $A_1, \dots A_s$ such that $G = A_1 + \cdots + A_s$. Then the following conditions are equivalent:*

(a) $(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$ *is an isomorphism of* $A_1 \times \cdots \times A_s$ *onto* G.

(b) *Each element* $g \in G$ *can be expressed as a sum* $x = a_1 + \cdots + a_s$, *with* $a_i \in A_i$ *for all* i, *in exactly one way.*

(c) *If* $0 = a_1 + \cdots + a_s$, *with* $a_i \in A_i$ *for all* i, *then* $a_i = 0$ *for all* i.

Proof. This can be obtained from results about direct products for general (not necessarily abelian) groups, but the proof for abelian groups is very direct. The map in part (a) is a homomorphism, because the groups are abelian. (Check this.) By hypothesis the homomorphism is surjective, so (a) is equivalent to the injectivity of the map. But (b) also states that the map is injective, and (c) states that the kernel of the map is trivial. So all three assertions are equivalent. ∎

Let G be a finite abelian group. For each prime number p define

$$G[p] = \{g \in G : o(g) \text{ is a power of } p\}.$$

It is straightforward to check that $G[p]$ is a subgroup of G. Note that $x \in G[p] \Leftrightarrow p^j x = 0$ for some $j \Leftrightarrow p^r x = 0$, where p^r is the largest power of p dividing the order of the group. $G[p] = \{0\}$ if p does not divide the order of G.

The first step in our analysis of finite abelian groups is to show that G is the (internal) direct product of the subgroups $G[p]$ for p dividing the order of G.

Theorem 3.3.2. *Let G be a finite abelian group and let $p_1, \dots, p_k$ be the primes dividing $|G|$. Then $G \cong G[p_1] \times \cdots \times G[p_k]$.*

Proof. Write $n = |G|$, and let $p_1^{k_1} \cdots p_s^{k_s}$ be the prime decomposition of n.

For each index i let $r_i = n/p_i^{k_i}$; that is, r_i is the largest divisor of n that is relatively prime to p_i. For all $x \in G$, we have $r_i x \in G[p_i]$, because $p_i^{k_i}(r_i x) = nx = 0$. Furthermore, if $x \in G[p_j]$ for some $j \neq i$, then $r_i x = 0$, because $p_j^{k_j}$ divides r_i.

The greatest common divisor of $\{r_1, \dots, r_s\}$ is 1. Therefore, there exist $t_1, \dots, t_s$ such that $t_1 r_1 + \cdots + t_s r_s = 1$. Hence for any $x \in G$, $x = 1x = t_1 r_1 x + \cdots + t_s r_s x \in G[p_1] + G[p_2] + \cdots + G[p_s]$. Thus $G = G[p_1] + \cdots + G[p_s]$.

Suppose that $x_j \in G[p_j]$ for $1 \leq j \leq s$ and $\sum_j x_j = 0$. Fix an index i. Since $r_i x_j = 0$ for $j \neq i$, we have

$$0 = r_i(\sum_j x_j) = \sum_j r_i x_j = r_i x_i.$$

Because r_i is relatively prime to the order of each nonzero element of $G[p_i]$, it follows that $x_i = 0$. Thus by Proposition 3.3.1 $G = G[p_1] \times \cdots \times G[p_s]$. ■

The following lemma is the most subtle item in this section. You might prefer to skip the proof on the first reading.

Lemma 3.3.3. *Let G be a finite abelian group. Let m denote the maximum of the orders of elements of G, and let $a \in G$ be an element order m. Let $\pi : G \longrightarrow G/\langle a \rangle$ be the quotient map. For every $\bar{b} \in G/\langle a \rangle$, there is an element $b \in G$ such that $\pi(b) = \bar{b}$, and $o(b) = o(\bar{b})$.*

Proof. Denote the order of $\bar{b}$ in $G/\langle a \rangle$ by r. Let b_1 be any element of B such that $\pi(b_1) = \bar{b}$; this is possible because π is surjective. Then

$$o(b_1)\bar{b} = o(b_1)\pi(b_1) = \pi(o(b_1)b_1) = \pi(0) = 0;$$

therefore, r divides the order of b_1. On the other hand, $o(b_1) \leq m$ by hypothesis.

Since $0 = r\bar{b} = \pi(rb_1)$, we have $rb_1 \in \langle a \rangle$, say $rb_1 = na$ for some integer n with $0 \leq n \leq m-1$.

I claim that n is divisible by r, say $n = qr$. Assuming this for the moment, we have $rb_1 = rqa$, or $r(b_1 - qa) = 0$. So, putting $b = b_1 - qa$, we have $\pi(b) = \pi(b_1) = \bar{b}$, and $rb = 0$; therefore, $o(b)|r$. On the other hand, because $\pi(b) = \bar{b}$, we have $r|o(b)$ (just as for b_1). It follows that $o(b) = r$, as desired.

It remains to show that n is divisible by r. Write $n = qr + s$ with $0 \leq s < r$. Then $rb_1 = qra + sa$, or $r(b_1 - qa) = sa$. We have to show that $s = 0$. Assume $s > 0$, in order to reach a contradiction.

Again, set $b = b_1 - qa$, so $\pi(b) = \pi(b_1) = \bar{b}$. We know that $o(sa) = m/\alpha$, where $\alpha = \text{g.c.d.}(s, m)$, by Proposition 2.2.33. Since $o(b)$ is divisible by r,

$$o(b) = r\,o(rb) = r\,o(sa) = r\,(m/\alpha) \geq rm/s > m.$$

Since $o(b) \leq m$, this is a contradiction. ■

Proposition 3.3.4. *Let G be a finite abelian group. Then G is a direct product of cyclic groups.*

Proof. We prove this by induction on the order of the abelian group, there being nothing to prove if $|G| = 1$. So assume $|G| > 1$ and that the assertion holds for all finite abelian groups of size strictly less than $|G|$. Let a_1 be an element of G of maximum order $r_1 > 1$ and put $A_1 = \langle a_1 \rangle$.

Applying the induction hypothesis to G/A_1, suppose that G/A_1 is a direct product of subgroups $\bar{A}_2, \bar{A}_3, \ldots, \bar{A}_k$, where $\bar{A}_i = \langle \bar{a}_i \rangle$ is cyclic of order r_i for $2 \leq i \leq k$. Let $\pi : G \longrightarrow G/A_1$ be the quotient map. Using Lemma 3.3.3, let a_i be a pre-image of $\bar{a}_i$ of order r_i for each i, $2 \leq i \leq k$, and let $A_i = \langle a_i \rangle$. We will show that $G = A_1 \times A_2 \times \cdots A_k$.

For each $g \in G$, there exist n_i for $2 \leq i \leq k$ such that $\pi(g) = \sum_{i \geq 2} n_i \bar{a}_i$. Thus, $g - \sum_{i \geq 2} n_i a_i \in A_1 = \langle a_i \rangle$, so there is an n_1 such that $g = \sum_{i \geq 1} n_i a_i$. This shows that $G = A_1 + A_2 + \cdots + A_k$.

Since each a_i has order r_i, an arbitrary element of A_i can be written as $n_i a_i$, with $0 \leq n_i < r_i$. Suppose a sum of such elements is zero: $\sum_{i \geq 1} n_i a_i = 0$. Applying π gives $\sum_{i \geq 2} n_i \bar{a}_i = 0$. Since G/A_1 is the internal direct product of the subgroups $\bar{A}_i = \langle \bar{a}_i \rangle$ for $2 \leq i \leq k$, it follows from Proposition 3.3.1 that $n_i \bar{a}_i = 0$ for $i \geq 2$. Because the order of $\bar{a}_i$ is r_i and $0 \leq n_i < r_i$, we have $n_i = 0$ for $i \geq 2$. Hence also $n_i a_i = 0$ for $i \geq 2$, and, therefore, $n_1 a_1 = 0$ as well.

By Proposition 3.3.1, G is the direct product of the subgroups A_i, $1 \leq i \leq k$. ∎

Corollary 3.3.5. *If G is a finite abelian group and p is a prime dividing the order of G, then G has an element of order p.*

Proof. Since G is a direct product of cyclic groups, p divides the order of some cyclic subgroup C of G, and C has an element of order p by Proposition 2.2.32. ∎

Corollary 3.3.6. *If G is a finite abelian group, then for each prime p, the order of $G[p]$ is the largest power of p dividing $|G|$.*

Proof. $G[p]$ has, by definition, no element of order q, where q is a prime different from p. Therefore, by the previous corollary, the order of $G[p]$ is a power of p. Since $|G| = \prod_p |G[p]|$, it follows that $|G[p]|$ is the largest power of p dividing $|G|$. ∎

Corollary 3.3.7. *Any finite abelian group is a direct product of cyclic groups, each of which has order a power of a prime.*

Proof. A finite abelian group G is a direct product of its subgroups $G[p]$. Each $G[p]$ is in turn a direct product of cyclic groups by Proposition 3.3.4, which must each be of order a power of p by Corollary 3.3.6 and Lagrange's theorem. ■

We can now obtain a complete structure theorem for abelian groups whose order is a power of a prime.

Theorem 3.3.8.

(a) *Let G be an abelian group of order p^n, where p is a prime. There exist natural numbers $n_1 \geq n_2 \geq \cdots \geq n_s$ such that $\sum_i n_i = n$, and $G \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_s}}$.*

(b) *The sequence of exponents in part (b) is unique. That is, if $m_1 \geq m_2 \geq \cdots \geq m_r$, $\sum_j m_j = n$, and $G \cong \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_r}}$, then $s = r$ and $n_i = m_i$ for all i.*

Proof. By Proposition 3.3.4, G is a direct product of cyclic groups, each of which must have order a power of p by Lagrange's theorem. This gives (a).

We prove the uniqueness statement (b) by induction on n, the case $n = 1$ being trivial. So suppose the uniqueness statement holds for all abelian groups of order $p^{n'}$ where $n' < n$. Consider the homomorphism $\varphi(x) = x^p$ of G into itself. Suppose

$$(n_1, \ldots, n_s) = (n_1, \ldots, n_{s'}, 1, 1, \ldots, 1)$$

and

$$(m_1, \ldots, m_r) = (m_1, \ldots, m_{r'}, 1, 1, \ldots, 1),$$

where $n_{s'} > 1$ and $n_{r'} > 1$. Then the isomorphism

$$G \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_s}}$$

gives

$$\varphi(G) \cong \mathbb{Z}_{p^{n_1-1}} \times \cdots \times \mathbb{Z}_{p^{n_{s'}-1}},$$

and the isomorphism

$$G \cong \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_r}}$$

gives

$$\varphi(G) \cong \mathbb{Z}_{p^{m_1-1}} \times \cdots \times \mathbb{Z}_{p^{m_{r'}-1}}.$$

The first isomorphism yields

$$\log_p |\varphi(G)| = \sum_{i=1}^{s'} (n_i - 1) = \sum_{i=1}^{s} (n_i - 1) = n - s,$$

and similarly the second isomorphism yields $\log_p |\varphi(G)| = n - r$. In particular, $r = s$. Now applying the induction hypothesis to $\varphi(G)$ gives also $s' = r'$ and $n_i - 1 = m_i - 1$ for $1 \leq i \leq s'$. This implies $n_i = m_i$ for $1 \leq i \leq s$. ∎

Example 3.3.9. Every abelian groups of order 32 is isomorphic to one of the following: $\mathbb{Z}_{32}$, $\mathbb{Z}_{16} \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_4$, $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let G be an abelian group of order p^n. There exist uniquely determined natural numbers $n_1 \geq n_2 \geq \cdots \geq n_s$ such that $\sum_i n_i = n$, and $G \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_s}}$. The sequence $(n_1, \ldots, n_s)$ is called the *type* of G. The type of an abelian group of prime power order determines the group up to isomorphism; two groups each of which have order a power of p are isomorphic if, and only if, they have the same type.

Example 3.3.10. A *partition* of a natural number n is a sequence of natural numbers $n_1 \geq n_2 \geq \cdots \geq n_s$ such that $\sum_i n_i = n$. The type of an abelian group of order p^n is a partition of n, and the number of different isomorphism classes of abelian groups of order p^n is the number of partitions of n. (The number does not depend on p.) For example, the distinct partitions of 7 are (7), (6, 1), (5, 2), (5, 1, 1), (4, 3), (4, 2, 1), (4, 1, 1, 1), (3, 3, 1), (3, 2, 2), (3, 2, 1, 1), (3, 1, 1, 1, 1), (2, 2, 2, 1), (2, 2, 1, 1, 1), (2, 1, 1, 1, 1, 1), and (1, 1, 1, 1, 1, 1, 1). So there are 15 different isomorphism classes of abelian groups of order p^7 for any prime p.

Lemma 3.3.11. *Suppose a finite abelian group G is an internal direct product of a collection $\{C_i\}$ of cyclic subgroups. Then for each prime p, the sum of those C_i whose order is a power of p is equal to $G[p]$.*

Proof. Denote by $A[p]$ the sum of those C_i whose order is a power of p. Then $A[p] \subseteq G[p]$ and G is the internal direct product of the subgroups $A[p]$. Since G is also the internal direct product of the subgroups $G[p]$, it follows that $A[p] = G[p]$ for all p. ∎

Example 3.3.12. Consider $G = \mathbb{Z}_{30} \times \mathbb{Z}_{50} \times \mathbb{Z}_{28}$. Then

$$\begin{aligned} G &\cong (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_{25} \times \mathbb{Z}_2) \times (\mathbb{Z}_4 \times \mathbb{Z}_7) \\ &\cong (\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \times (\mathbb{Z}_{25} \times \mathbb{Z}_5) \times \mathbb{Z}_7. \end{aligned}$$

Thus $G[2] \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $G[3] \cong \mathbb{Z}_3$, $G[5] \cong \mathbb{Z}_{25} \times \mathbb{Z}_5$, and $G[7] \cong \mathbb{Z}_7$. $G[p] = 0$ for all other primes p.

Theorem 3.3.13. *(Fundamental theorem of finite abelian groups). Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. The number of cyclic groups of each order appearing in such a direct product decomposition is uniquely determined, and, moreover, determines the group up to isomorphism.*

Proof. Let G be a finite abelian group. By Corollary 3.3.7, G is isomorphic to a direct product of cyclic groups of prime power order. Suppose $\{C_i : 1 \le i \le N\}$ and $\{D_j : 1 \le j \le M\}$ are two families of cyclic subgroups of G of prime power order such that

$$G = C_1 \times \cdots \times C_N = D_1 \times \cdots \times D_M.$$

Group each family of cyclic subgroups according to the primes dividing $|G|$,

$$\{C_i\} = \bigcup_p \{C_i^p : 1 \le i \le N(p)\}, \quad \text{and}$$

$$\{D_j\} = \bigcup_p \{D_j^p : 1 \le j \le M(p)\},$$

where each C_i^p and D_j^p has order a power of p. According to the previous lemma, $\sum_{i=1}^{N(p)} C_i^p = \sum_{j=1}^{M(p)} D_j^p = G[p]$ for each prime p dividing $|G|$. It follows from Theorem 3.3.8 and Corollary 3.3.6 that $N(p) = M(p)$ and

$$\{|C_i^p| : 1 \le i \le N(p)\} = \{|D_j^p| : 1 \le j \le N(p)\}.$$

It follows that $M = N$ and $\{|C_i| : 1 \le i \le N\} = \{|D_j| : 1 \le j \le N\}$. ■

Example 3.3.14. Consider the example $G = \mathbb{Z}_{30} \times \mathbb{Z}_{50} \times \mathbb{Z}_{28}$ again. The unique decomposition of G into cyclic groups of prime power order is

$$G \cong (\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \times (\mathbb{Z}_{25} \times \mathbb{Z}_5) \times \mathbb{Z}_7.$$

Another canonical direct product decomposition is obtained by regrouping the factors as follows:

$$\begin{aligned} G &\cong (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_7) \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times \mathbb{Z}_2 \\ &\cong \mathbb{Z}_{4\cdot 3\cdot 25\cdot 7} \times \mathbb{Z}_{2\cdot 5} \times \mathbb{Z}_2 \\ &\cong \mathbb{Z}_{2100} \times \mathbb{Z}_{10} \times \mathbb{Z}_2. \end{aligned}$$

Corollary 3.3.15. *If G is a finite abelian group, there exist unique natural numbers $m_1, m_2, \ldots, m_r$ such that $m_i \geq 2$, m_{i+1} divides m_i for all i and $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$.*

Proof. Exercise 3.3.6. ■

Corollary 3.3.16. *If G is a finite abelian group and m is the maximum of orders of elements of G, then the order of any element of G divides m.*

Proof. Exercise 3.3.8. ■

Corollary 3.3.17. *Let K be a finite field of order n. Then the multiplicative group of units of K is cyclic of order $n-1$. In particular, for p a prime number, the multiplicative group $\Phi(p)$ of units of $\mathbb{Z}_p$ is cyclic of order $p-1$.*

Proof. Let K^* denote the multiplicative group of nonzero elements of K. Then K^* is abelian of order $n-1$. Let m denote the maximum of the orders of elements of K^*. We want to show that $m = n-1$. On the one hand, $m \leq n-1$, since every element has order dividing the order of the group. On the other hand, according to Corollary 3.3.16, $x^m = 1$ for all elements $x \in K^*$, so that the equation $x^m - 1 = 0$ has $n-1$ distinct solutions in the field K. But the number of distinct roots of a polynomial in a field is never more than the degree of the polynomial (Corollary 1.8.25), so $n-1 \leq m$. ■

Remark 3.3.18. Note that while the proof insures that the group of units of K^* is cyclic, it does not provide a means of actually *finding* a generator! In particular, it is not obvious how to find a nonzero element of $\mathbb{Z}_p$ of multiplicative order $p-1$.

The rest of this section is devoted to working out the structure of the group $\Phi(N)$ of units in $\mathbb{Z}_N$. Recall that $\Phi(N)$ has order $\varphi(N)$,

where φ is the Euler φ function. We have just determined that for a prime p, $\Phi(p)$ is cyclic of order $p-1$.

Proposition 3.3.19.

(a) *If* N *has prime decomposition* $N = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, *then*

$$\Phi(N) \cong \Phi(p_1^{k_1}) \times \Phi(p_2^{k_2}) \times \cdots \times \Phi(p_s^{k_s}).$$

(b) $\Phi(2)$ *and* $\Phi(4)$ *are cyclic.* $\Phi(2^n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ *if* $n \geq 3$.

(c) *If* p *is an odd prime, then for all* n, $\Phi(p^n) \cong \mathbb{Z}_{p^{n-1}(p-1)} \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p-1}$.

Proof. You are asked to prove part (a) in Exercise 3.3.9.

The groups $\Phi(2)$ and $\Phi(4)$ are of orders 1 and 2, respectively, so they are necessarily cyclic. For $n \geq 3$, we have already seen in Example 2.2.34 that $\Phi(2^n)$ is not cyclic and that $\Phi(2^n)$ contains three distinct elements of order 2, and in Exercise 2.2.30 that $[3]$ has order 2^{n-1} in $\Phi(2^n)$. The cyclic subgroup $\langle[3]\rangle$ contains exactly one of the three elements of order 2. If a is an element of order 2 *not* contained in $\langle[3]\rangle$, then $\langle a\rangle \cap \langle[3]\rangle = [1]$, so the subgroup generated by $\langle a\rangle$ and $\langle[3]\rangle$ is a direct product, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-1}}$. Because $|\Phi(2^n)| = |\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-1}}| = 2^{n-1}$, we have $\Phi(2^n) = \langle a\rangle \times \langle[3]\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-1}}$. This completes the proof of part (b).

Now let p be an odd prime, and let $n \geq 1$. Lemma 3.3.17 already shows that $\Phi(p^n)$ is cyclic when $n = 1$, so we can assume $n \geq 2$.

Using Lemma 3.3.17, we obtain a natural number a such that $a^{p-1} \equiv 1 \pmod{p}$ and $a^\ell \not\equiv 1 \pmod{p}$ for $\ell < p-1$.

We claim that the order of $[a^{p^{n-1}}]$ in $\Phi(p^n)$ is $(p-1)$. In any case, $(a^{p^{n-1}})^{p-1} = a^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$ so the order ℓ of $[a^{p^{n-1}}]$ divides $p-1$. But we have $a^p \equiv a \pmod{p}$, so $a^{p^{n-1}} \equiv a \pmod{p}$, and $a^{p^{n-1}\ell} \equiv a^\ell \pmod{p}$. If $\ell < p-1$, then $a^{p^{n-1}\ell} \equiv a^\ell$ is not congruent to 1 modulo p, so it is not congruent to 1 modulo p^n. Therefore, the order of $[a^{p^{n-1}}]$ is $p-1$ as claimed.

It follows from Exercise 1.9.10 that the order of $[p+1]$ in $\Phi(p^n)$ is p^{n-1}.

We now have elements $x = [a^{p^{n-1}}]$ of order $p-1$ and $y = [p-1]$ of order p^{n-1} in $\Phi(p^n)$. Since the orders of x and y are relatively prime, the order of the product xy is the product of the orders $p^{n-1}(p-1)$. Thus $\Phi(p^n)$ is cyclic.

Another way to finish the proof of part (c) is to observe that $\langle x\rangle \cap \langle y\rangle = \{1\}$, since the orders of these cyclic subgroups are relatively prime. It follows then that the subgroup generated by x and y is the direct product $\langle x\rangle \times \langle y\rangle \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{n-1}} \cong \mathbb{Z}_{p^{n-1}(p-1)}$. ∎

Remark 3.3.20. All of the isomorphisms here are explicit, as long as we are able to find a generator for $\Phi(p)$ for all primes p appearing in the decompositions.

Exercises 3.3

3.3.1. Find all abelian groups of order 108.

3.3.2. Find all abelian groups of order 144.

3.3.3. How many abelian groups are there of order 128, up to isomorphism?

3.3.4. How many abelian groups are there of order p^5q^4, where p and q are distinct primes?

3.3.5. Show that $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic if $\text{g.c.d.}(a, b) \geq 2$.

3.3.6. Prove Corollary 3.3.15. Hint: You need to work out how the m_i are related to the orders of the cyclic groups of prime power order appearing in the fundamental theorem. The uniqueness follows because the m_i and the orders of the cyclic groups of prime power order determine one another.

3.3.7. Determine the decomposition $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ given in the last exercise for finite abelian groups G or order 108 and 144.

3.3.8. Prove Corollary 3.3.16.

3.3.9. Recall that if a and b are relatively prime natural numbers, then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ as rings.

(a) If a, b are relatively prime natural numbers, show that the ring isomorphism $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ implies that $\Phi(ab) \cong \Phi(a) \times \Phi(b)$.

(b) Show that if $N = p_1^{k_1} \cdots p_s^{k_s}$ is the prime decomposition of N, then
$$\Phi(N) \cong \Phi(p_1^{k_1}) \times \cdots \times \Phi(p_s^{k_s}).$$

(c) Since these group isomorphisms are obtained independently of our earlier computations of $\varphi(N)$, show that we can recover the multiplicativity of the Euler φ function from the group theory results. Namely, conclude from from parts (a) - (c) that $\varphi(ab) = \varphi(a)\varphi(b)$ if a, b are relatively prime, and that if $N = p_1^{k_1} \cdots p_s^{k_s}$, then $\varphi(N) = \prod_i \varphi(p_i^{k_i})$.

3.3.10. Find the structure of the group $\Phi(n)$ for $n \leq 20$.