Modern Algebra

Chapter II. The Structure of Groups

II.2. Finitely Generated Abelian Groups—Proofs of Theorems

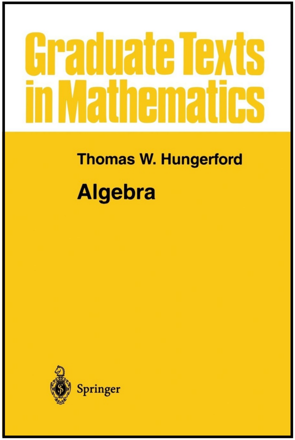

Table of contents

Theorem II.2.1

Theorem II.2.1. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, m_2, \ldots, m_t$ where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Proof. If $G \neq \{0\}$ and G is generated by n elements then there is a free abelian group F of rank n and an onto homomorphism (epimorphism) $\pi : F \to G$ by Theorem II.1.4. If π is an isomorphism then $G \cong F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands) by Theorem II.1.1(iii).

Theorem II.2.1

Theorem II.2.1. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, m_2, \ldots, m_t$ where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Proof. If $G \neq \{0\}$ and G is generated by n elements then there is a free abelian group F of rank n and an onto homomorphism (epimorphism) $\pi : F \to G$ by Theorem II.1.4. If π is an isomorphism then $G \cong F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands) by Theorem II.1.1(iii). If π is not an isomorphism then by Theorem II.1.6 there is a basis $\{x_1, x_2, \ldots, x_n\}$ of F and positive integers $d_1, d_2, \ldots, d_r$ such that $1 \leq r \leq n$, $d_1 \mid d_2 \mid \cdots \mid d_r$ and $\{d_1x_1, d_2x_2, \ldots, d_rx_r\}$ is a basis of $K = \mathrm{Ker}(\pi)$ (here, G of Theorem II.1.6 is $\mathrm{Ker}(\pi)$). Now $F = \sum_{i=1}^n \langle x_i \rangle$ (direct sum) and $K = \sum_{i=1}^r \langle d_i x_i \rangle$, where $\langle x_i \rangle \cong \mathbb{Z}$ by Theorem II.1.1(iii)) and under the same isomorphism between $\langle x_i \rangle$ and $\mathbb{Z}$ we have $\langle d_i x_i \rangle \cong d_i\mathbb{Z} = \{d_i u \mid u \in \mathbb{Z}\}$.

Theorem II.2.1

Theorem II.2.1. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, m_2, \ldots, m_t$ where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Proof. If $G \neq \{0\}$ and G is generated by n elements then there is a free abelian group F of rank n and an onto homomorphism (epimorphism) $\pi : F \to G$ by Theorem II.1.4. If π is an isomorphism then $G \cong F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands) by Theorem II.1.1(iii). If π is not an isomorphism then by Theorem II.1.6 there is a basis $\{x_1, x_2, \ldots, x_n\}$ of F and positive integers $d_1, d_2, \ldots, d_r$ such that $1 \leq r \leq n$, $d_1 \mid d_2 \mid \cdots \mid d_r$ and $\{d_1x_1, d_2x_2, \ldots, d_rx_r\}$ is a basis of $K = \mathrm{Ker}(\pi)$ (here, G of Theorem II.1.6 is $\mathrm{Ker}(\pi)$). Now $F = \sum_{i=1}^{n} \langle x_i \rangle$ (direct sum) and $K = \sum_{i=1}^{r} \langle d_i x_i \rangle$, where $\langle x_i \rangle \cong \mathbb{Z}$ by Theorem II.1.1(iii)) and under the same isomorphism between $\langle x_i \rangle$ and $\mathbb{Z}$ we have $\langle d_i x_i \rangle \cong d_i\mathbb{Z} = \{d_i u \mid u \in \mathbb{Z}\}$.

Theorem II.2.1 (continued 1)

Proof (continued). For $i = r+1, r+2, \ldots, n$ let $d_i = 0$ so that $K = \sum_{i=1}^{n} \langle d_i x_i \rangle$. Then

$$\begin{aligned} G &\cong F/K \text{ by Corollary I.5.7 (First Isomorphism Theorem)} \\ &= \sum_{i=1}^{n} \langle x_i \rangle \Big/ \sum_{i=1}^{n} \langle d_i x_i \rangle \\ &\cong \sum_{i=1}^{n} \langle x_i \rangle / \langle d_i x_i \rangle \text{ by Corollary I.8.11} \\ &\cong \sum_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \text{ by Corollary I.5.8.} \end{aligned}$$

If $d_i = 1$, then $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{0\}$. If $d_i > 1$, then $\mathbb{Z}/d_i\mathbb{Z} \cong \mathbb{Z}_{d_i}$. If $d_i = 0$ then $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$.

Theorem II.2.1 (continued 2)

Theorem II.2.1. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, m_2, \ldots, m_t$ where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Proof (continued). Let $m_1, m_2, \ldots, m_t$ be those d_i (in increasing order) such that $d_i \not\in \{0, 1\}$ and let s be the number of d_i such that $d_i = 0$. Then

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z})$$

where $m_1 > 1$ (since values of 0 and 1 are omitted), $m_1 \mid m_2 \mid \cdots \mid m_t$ (since $d_1 \mid d_2 \mid \cdots \mid d_r$ and the m_i's <u>are</u> some of the d_j's) and $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ has rank s (with the obvious basis). □

Lemma II.2.3

Lemma II.2.3. If m is a positive integer and $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ $(p_a, p_2, \ldots, p_t$ distinct primes and each $n_i \in \mathbb{N})$, then

$$\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{n_1}} \oplus \mathbb{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_t}^{n_t}}.$$

Proof. First, consider $\mathbb{Z}_{rn}$ where $r, n \in \mathbb{N}$ are relatively prime. The element $\overline{n} = n\overline{1} \in \mathbb{Z}_{rn}$ has order r by Theorem I.3.4(vii). Whence $\mathbb{Z}_r \cong \langle n\overline{1} \rangle < \mathbb{Z}_{rn}$ and the map $\psi_1 : \mathbb{Z}_r \to \mathbb{Z}_{rn}$ defined by $\overline{k} \mapsto n\overline{k}$ is a one to one homomorphism ("monomorphism"). Similarly, $\psi_2 : \mathbb{Z}_n \to \mathbb{Z}_{rn}$ given by $\overline{k} \mapsto r\overline{k}$ is a one to one homomorphism.

Lemma II.2.3

Lemma II.2.3. If m is a positive integer and $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ($p_a, p_2, \ldots, p_t$ distinct primes and each $n_i \in \mathbb{N}$), then

$$\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{n_1}} \oplus \mathbb{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_t}^{n_t}}.$$

Proof. First, consider $\mathbb{Z}_{rn}$ where $r, n \in \mathbb{N}$ are relatively prime. The element $\overline{n} = n\overline{1} \in \mathbb{Z}_{rn}$ has order r by Theorem I.3.4(vii). Whence $\mathbb{Z}_r \cong \langle n\overline{1} \rangle < \mathbb{Z}_{rn}$ and the map $\psi_1 : \mathbb{Z}_r \to \mathbb{Z}_{rn}$ defined by $\overline{k} \mapsto n\overline{k}$ is a one to one homomorphism ("monomorphism"). Similarly, $\psi_2 : \mathbb{Z}_n \to \mathbb{Z}_{rn}$ given by $\overline{k} \mapsto r\overline{k}$ is a one to one homomorphism. As seen in the proof of Theorem I.8.5, the map $\psi : \mathbb{Z}_r \oplus \mathbb{Z}_n \to \mathbb{Z}_{rn}$ given by $(\overline{x}, \overline{y}) \mapsto \psi_1(\overline{x}) + \psi_2(\overline{y}) = n\overline{x} + r\overline{y}$ is a well-defined homomorphism. Since r and n are relatively prime then $ra + nb = 1$ for some $a, b \in \mathbb{Z}$ by Theorem 0.6.5. Hence for $\overline{k} \in \mathbb{Z}_{rn}$ we have $\overline{k} = ra\overline{k} + nb\overline{k} = \psi(b\overline{k}, a\overline{k})$ and ψ is onto. Since $|\mathbb{Z}_r \oplus \mathbb{Z}_n| = rn = |\mathbb{Z}_{rn}|$ and so ψ is one to one. So the lemma holds for $t = 2$. It now follows for general $t \in \mathbb{N}$ by induction. $\square$

Lemma II.2.3

Lemma II.2.3. If m is a positive integer and $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ($p_a, p_2, \ldots, p_t$ distinct primes and each $n_i \in \mathbb{N}$), then

$$\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{n_1}} \oplus \mathbb{Z}_{{p_2}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_t}^{n_t}}.$$

Proof. First, consider $\mathbb{Z}_{rn}$ where $r, n \in \mathbb{N}$ are relatively prime. The element $\overline{n} = n\overline{1} \in \mathbb{Z}_{rn}$ has order r by Theorem I.3.4(vii). Whence $\mathbb{Z}_r \cong \langle n\overline{1} \rangle < \mathbb{Z}_{rn}$ and the map $\psi_1 : \mathbb{Z}_r \to \mathbb{Z}_{rn}$ defined by $\overline{k} \mapsto n\overline{k}$ is a one to one homomorphism ("monomorphism"). Similarly, $\psi_2 : \mathbb{Z}_n \to \mathbb{Z}_{rn}$ given by $\overline{k} \mapsto r\overline{k}$ is a one to one homomorphism. As seen in the proof of Theorem I.8.5, the map $\psi : \mathbb{Z}_r \oplus \mathbb{Z}_n \to \mathbb{Z}_{rn}$ given by $(\overline{x}, \overline{y}) \mapsto \psi_1(\overline{x}) + \psi_2(\overline{y}) = n\overline{x} + r\overline{y}$ is a well-defined homomorphism. Since r and n are relatively prime then $ra + nb = 1$ for some $a, b \in \mathbb{Z}$ by Theorem 0.6.5. Hence for $\overline{k} \in \mathbb{Z}_{rn}$ we have $\overline{k} = ra\overline{k} + nb\overline{k} = \psi(b\overline{k}, a\overline{k})$ and ψ is onto. Since $|\mathbb{Z}_r \oplus \mathbb{Z}_n| = rn = |\mathbb{Z}_{rn}|$ and so ψ is one to one. So the lemma holds for $t = 2$. It now follows for general $t \in \mathbb{N}$ by induction. $\square$

Lemma II.2.A

Lemma II.2.A. If m is a positive integer and $m = nk$ where n and k are not relatively prime, then $\mathbb{Z}_m \ncong \mathbb{Z}_n \oplus \mathbb{Z}_k$.

Proof. Let $d = \gcd(n, k)$. By hypothesis, $d > 1$. So nk/d is divisible by both n and k, and $nk/d < nk$. If $(r, s) \in \mathbb{Z}_n \oplus \mathbb{Z}_k$ then $(nk/d)(r, s) = (\overline{0}, \overline{0})$ by Theorem I.3.4(iv). So the order of (r, s) is at most nk/d (by Theorem I.3.4(iii)). But $nk/d < nk = |\mathbb{Z}_n \oplus \mathbb{Z}_k|$. So no element of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ generates $\mathbb{Z}_n \oplus \mathbb{Z}_k$ and hence $\mathbb{Z}_n \oplus \mathbb{Z}_k$ is not cyclic. So $\mathbb{Z}_m \ncong \mathbb{Z}_n \oplus \mathbb{Z}_k$. □

Lemma II.2.A

Lemma II.2.A. If m is a positive integer and $m = nk$ where n and k are not relatively prime, then $\mathbb{Z}_m \ncong \mathbb{Z}_n \oplus \mathbb{Z}_k$.

Proof. Let $d = \gcd(n, k)$. By hypothesis, $d > 1$. So nk/d is divisible by both n and k, and $nk/d < nk$. If $(r, s) \in \mathbb{Z}_n \oplus \mathbb{Z}_k$ then $(nk/d)(r, s) = (\overline{0}, \overline{0})$ by Theorem I.3.4(iv). So the order of (r, s) is at most nk/d (by Theorem I.3.4(iii)). But $nk/d < nk = |\mathbb{Z}_n \oplus \mathbb{Z}_k|$. So no element of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ generates $\mathbb{Z}_n \oplus \mathbb{Z}_k$ and hence $\mathbb{Z}_n \oplus \mathbb{Z}_k$ is not cyclic. So $\mathbb{Z}_m \ncong \mathbb{Z}_n \oplus \mathbb{Z}_k$. □

Theorem II.2.2

Theorem II.2.2. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime.

Proof. By Theorem II.2.1 (see the proof)

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}).$$

By Lemma II.2.3, each $\mathbb{Z}_{m_i}$ can be written as a direct sum of cyclic groups each of order a power of a prime (the primes here may not be distinct in the representation of G). □

Theorem II.2.2

Theorem II.2.2. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime.

Proof. By Theorem II.2.1 (see the proof)

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}).$$

By Lemma II.2.3, each $\mathbb{Z}_{m_i}$ can be written as a direct sum of cyclic groups each of order a power of a prime (the primes here may not be distinct in the representation of G). $\square$

Corollary II.2.4

Corollary II.2.4. If G is a finite abelian group of order n, then G has a subgroup of order m for every positive integer m that divides n.

Proof. First, for some p and $\ell \in \mathbb{N}$, consider the cyclic group $\mathbb{Z}_{p^\ell}$. For all $k \in \mathbb{N}$ with $1 \leq k < \ell$, consider the subgroup of $\mathbb{Z}_{p^\ell}$ generated by $p^k\overline{1}$, $\langle p^k\overline{1}\rangle$. Since the order of $p^k\overline{1}$ is $p^{\ell-k}$:

$$\underbrace{P^k\overline{1} + p^k\overline{1} + \cdots + p^k\overline{1}}_{p^{\ell-k} \text{ times}} = p^\ell\overline{1} = \overline{0}.$$

So $\langle p^k\overline{1}\rangle$ is a cyclic group of order $p^{\ell-k}$ and hence is isomorphic to $\mathbb{Z}_{p^{\ell-k}}$. Hence

$$\mathbb{Z}_{p^\ell} \text{ has a subgroup isomorphic to } \mathbb{Z}_{p^k} \text{ for } k = 1, 2, \ldots, \ell - 1 \quad (*)$$

(replacing $\ell - k$ with k here).

Corollary II.2.4

Corollary II.2.4. If G is a finite abelian group of order n, then G has a subgroup of order m for every positive integer m that divides n.

Proof. First, for some p and $\ell \in \mathbb{N}$, consider the cyclic group $\mathbb{Z}_{p^\ell}$. For all $k \in \mathbb{N}$ with $1 \le k < \ell$, consider the subgroup of $\mathbb{Z}_{p^\ell}$ generated by $p^k\overline{1}$, $\langle p^k\overline{1}\rangle$. Since the order of $p^k\overline{1}$ is $p^{\ell-k}$:

$$\underbrace{P^k\overline{1} + p^k\overline{1} + \cdots + p^k\overline{1}}_{p^{\ell-k}\text{ times}} = p^\ell\overline{1} = \overline{0}.$$

So $\langle p^k\overline{1}\rangle$ is a cyclic group of order $p^{\ell-k}$ and hence is isomorphic to $\mathbb{Z}_{p^{\ell-k}}$. Hence

$$\mathbb{Z}_{p^\ell} \text{ has a subgroup isomorphic to } \mathbb{Z}_{p^k} \text{ for } k = 1, 2, \ldots, \ell - 1 \quad (*)$$

(replacing $\ell - k$ with k here).

Corollary II.2.4 (continued 1)

Proof (continued). This also follows from Theorem I.3.4(vii)—Hungerford uses Lemma II.2.5(v) which has not yet been shown but is next and is based on Theorem I.3.4(vii).

By Theorem II.2.2, $G = \sum_{i=1}^{k} G_i$ where each G_i is a finite cyclic group and so by Lemma II.2.3 is of the form

$$\mathbb{Z}_{m'} \cong \mathbb{Z}_{p_1^{m'_1}} \oplus \mathbb{Z}_{p_2^{m'_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{m'_t}}$$

for distinct primes $p_1, p_2, \ldots, p_t$.

Now for any m dividing n, we have that for $n = p_1^{n_1} p_2^{n_2} \cdots p_j^{n_j}$ (distinct primes) then m must be of the form $m = p_1^{m_1} p_2^{m_2} \cdots p_j^{m_j}$ (some of the exponents here may be 0). Now $|G| = |G_1||G_2| \cdots |G_k|$ so for any $p_i^{m_i} \mid n$, some of the G_r's must have subgroups of order some positive power of p_i; the totality of these subgroups yields a subgroup of G of the form

$$\mathbb{Z}_{p_i^{n'_1}} \oplus \mathbb{Z}_{p_i^{n'_2}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{n'_r}}.$$

Corollary II.2.4 (continued 1)

Proof (continued). This also follows from Theorem I.3.4(vii)—Hungerford uses Lemma II.2.5(v) which has not yet been shown but is next and is based on Theorem I.3.4(vii).
By Theorem II.2.2, $G = \sum_{i=1}^{k} G_i$ where each G_i is a finite cyclic group and so by Lemma II.2.3 is of the form

$$\mathbb{Z}_{m'} \cong \mathbb{Z}_{p_1^{m'_1}} \oplus \mathbb{Z}_{p_2^{m'_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{m'_t}}$$

for distinct primes $p_1, p_2, \ldots, p_t$.
Now for any m dividing n, we have that for $n = p_1^{n_1} p_2^{n_2} \cdots p_j^{n_j}$ (distinct primes) then m must be of the form $m = p_1^{m_1} p_2^{m_2} \cdots p_j^{m_j}$ (some of the exponents here may be 0). Now $|G| = |G_1||G_2| \cdots |G_k|$ so for any $p_i^{m_i} \mid n$, some of the G_r's must have subgroups of order some positive power of p_i; the totality of these subgroups yields a subgroup of G of the form

$$\mathbb{Z}_{p_i^{n'_1}} \oplus \mathbb{Z}_{p_i^{n'_2}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{n'_r}}.$$

Corollary II.2.4 (continued 2)

Corollary II.2.4. If G is a finite abelian group of order n, then G has a subgroup of order m for every positive integer m that divides n.

Proof (continued). By taking a sufficient number of these $\mathbb{Z}_{p_i^n}$'s along with an appropriate sized subgroup of one of the $\mathbb{Z}_{p_i^n}$'s (as necessary; this can be done by $(*)$ above), we get the subgroup of G of the form

$$\mathbb{Z}_{p_i^{n_1''}} \oplus \mathbb{Z}_{p_i^{n_2''}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{n_\alpha''}}$$

where $n_1'' + n_2'' + \cdots + n_\alpha'' = m_i$. Do this for each m_i ($i = 1, 2, \ldots, j$) and distinct prime p_i to produce a family of subgroups of G of each desired prime power order (notice that each of these intersects only at the identity) and take the direct sum of these (see Definition I.8.8). This is a subgroup of the desired order m. □

Lemma II.2.5

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. There are the following isomorphism relationships

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$ and $p^m\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$ $(m < n)$.

Proof of (v). The element $p^{n-1}\overline{1} = \overline{p^{n-1}} \in \mathbb{Z}_{p^n}$ has order p by Theorem I.3.4(vii), whence $\langle\overline{p^{n-1}}\rangle \cong \mathbb{Z}_p$ (by Theorem I.3.2) and $\langle\overline{p^{n-1}}\rangle < \mathbb{Z}_{p^n}[p]$. If $\overline{u} \in \mathbb{Z}_{p^n}[p]$ then $p\overline{u} = \overline{0}$ in $\mathbb{Z}_{p^n}$ (by definition of $\mathbb{Z}_{p^n}[p]$) so that $pu \equiv 0 \pmod{p}$ in $\mathbb{Z}$. But $p^n \mid pu$ implies $p^{n-1} \mid u$. Therefore in $\mathbb{Z}_{p^n}$ we have $\overline{u} \in \langle\overline{p^{n-1}}\rangle$ and $\mathbb{Z}_{p^n}[p] < \langle\overline{p^{n-1}}\rangle$. So we have that $\mathbb{Z}_{p^n}[p] = \langle p^{n-1}\rangle \cong \mathbb{Z}_p$ and the first claim holds.

Lemma II.2.5

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. There are the following isomorphism relationships

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$ and $p^m\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$ $(m < n)$.

Proof of (v). The element $p^{n-1}\overline{1} = \overline{p^{n-1}} \in \mathbb{Z}_{p^n}$ has order p by Theorem I.3.4(vii), whence $\langle\overline{p^{n-1}}\rangle \cong \mathbb{Z}_p$ (by Theorem I.3.2) and $\langle\overline{p^{n-1}}\rangle < \mathbb{Z}_{p^n}[p]$. If $\overline{u} \in \mathbb{Z}_{p^n}[p]$ then $p\overline{u} = \overline{0}$ in $\mathbb{Z}_{p^n}$ (by definition of $\mathbb{Z}_{p^n}[p]$) so that $pu \equiv 0 \pmod{p}$ in $\mathbb{Z}$. But $p^n \mid pu$ implies $p^{n-1} \mid u$. Therefore in $\mathbb{Z}_{p^n}$ we have $\overline{u} \in \langle\overline{p^{n-1}}\rangle$ and $\mathbb{Z}_{p^n}[p] < \langle\overline{p^{n-1}}\rangle$. So we have that $\mathbb{Z}_{p^n}[p] = \langle p^{n-1}\rangle \cong \mathbb{Z}_p$ and the first claim holds.

For the second statement, note that $\overline{p^m} \in \mathbb{Z}_{p^n}$ has order p^{n-m} by Theorem I.3.4(viii). Therefore $p^m\mathbb{Z}_{p^n} = \{p^m\overline{u} \mid \overline{u} \in \mathbb{Z}_{p^n}\} = \langle\overline{p^m}\rangle \cong \mathbb{Z}_{p^{n-m}}$ by Theorem I.3.2. □

Lemma II.2.5

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. There are the following isomorphism relationships

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$ and $p^m\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$ $(m < n)$.

Proof of (v). The element $p^{n-1}\overline{1} = \overline{p^{n-1}} \in \mathbb{Z}_{p^n}$ has order p by Theorem I.3.4(vii), whence $\langle \overline{p^{n-1}} \rangle \cong \mathbb{Z}_p$ (by Theorem I.3.2) and $\langle \overline{p^{n-1}} \rangle < \mathbb{Z}_{p^n}[p]$. If $\overline{u} \in \mathbb{Z}_{p^n}[p]$ then $p\overline{u} = \overline{0}$ in $\mathbb{Z}_{p^n}$ (by definition of $\mathbb{Z}_{p^n}[p]$) so that $pu \equiv 0 \pmod{p}$ in $\mathbb{Z}$. But $p^n \mid pu$ implies $p^{n-1} \mid u$. Therefore in $\mathbb{Z}_{p^n}$ we have $\overline{u} \in \langle \overline{p^{n-1}} \rangle$ and $\mathbb{Z}_{p^n}[p] < \langle \overline{p^{n-1}} \rangle$. So we have that $\mathbb{Z}_{p^n}[p] = \langle p^{n-1} \rangle \cong \mathbb{Z}_p$ and the first claim holds.

For the second statement, note that $\overline{p^m} \in \mathbb{Z}_{p^n}$ has order p^{n-m} by Theorem I.3.4(viii). Therefore $p^m\mathbb{Z}_{p^n} = \{p^m\overline{u} \mid \overline{u} \in \mathbb{Z}_{p^n}\} = \langle \overline{p^m} \rangle \cong \mathbb{Z}_{p^{n-m}}$ by Theorem I.3.2. $\square$

Lemma II.2.5 (continued 1)

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. Let H and G be abelian groups.

(vii) If $f : G \to H$ is an isomorphism then the restrictions of f to G_t and $G(p)$ respectively are isomorphisms giving

$$G_t \cong H_t \text{ and } G(p) \cong H(p).$$

Proof of (vii). If $f : G \to H$ is a homomorphism and $x \in G(p) = \{u \in G \mid |u| = p^n \text{ for some } n \geq 0\}$ then x is of order p^n and $p^n f(x) = f(p^n x) = f(0) = 0$. Therefore $f(x) \in H(p) = \{u \in H \mid |u| = p^n \text{ for some } n > 0\}$. Hence $f : G(p) \to H(p)$. If f is an isomorphism and $y \in H(p) = \{u \in H \mid |u| = p^n \text{ for some } n > 0\}$ then y is of order p^n and $p^n x = p^n f^{-1}(y) = f^{-1}(p^n y)$ (since f^{-1} is an isomorphism to; where $y = f(x)$) and $p^n y = 0$ so $p^n x = f^{-1}(0) = 0$, so $x \in G(P)$ and $f^{-1} : H(p) \to G(p)$.

Lemma II.2.5 (continued 1)

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. Let H and G be abelian groups.

(vii) If $f : G \to H$ is an isomorphism then the restrictions of f to G_t and $G(p)$ respectively are isomorphisms giving
$$G_t \cong H_t \text{ and } G(p) \cong H(p).$$

Proof of (vii). If $f : G \to H$ is a homomorphism and $x \in G(p) = \{u \in G \mid |u| = p^n \text{ for some } n \geq 0\}$ then x is of order p^n and $p^n f(x) = f(p^n x) = f(0) = 0$. Therefore $f(x) \in H(p) = \{u \in H \mid |u| = p^n \text{ for some } n > 0\}$. Hence $f : G(p) \to H(p)$. If f is an isomorphism and $y \in H(p) = \{u \in H \mid |u| = p^n \text{ for some } n > 0\}$ then y is of order p^n and $p^n x = p^n f^{-1}(y) = f^{-1}(p^n y)$ (since f^{-1} is an isomorphism to; where $y = f(x)$) and $p^n y = 0$ so $p^n x = f^{-1}(0) = 0$, so $x \in G(P)$ and $f^{-1} : H(p) \to G(p)$.

Lemma II.2.5 (continued 2)

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. Let H and G be abelian groups.

(vii) If $f : G \to H$ is an isomorphism then the restrictions of f to G_t and $G(p)$ respectively are isomorphisms giving

$$G_t \cong H_t \text{ and } G(p) \cong H(p).$$

Proof of (vii), continued.
Since $ff^{-1} = 1_{H(p)}$ and $f^{-1}f = 1_{G(P)}$, then f is bijective from $G(p)$ to $H(p)$ and hence is an isomorphism. That is, $G(p) \cong H(p)$.
The proof that $G_t \cong H_t$ is similar to the above argument, but "p^n for some n" is simply replaced with some (finite) $n \in \mathbb{N}$. $\square$

Theorem II.2.6

Theorem II.2.6. Fundamental Theorem of Finitely Generated Abelian Groups.
Let G be a finitely generated abelian group.

(i) There is a unique nonnegative integer s such that the number of infinite cyclic summands in any decomposition of G as a direct sum of cyclic groups is precisely s.

Proof of (i). Any decomposition of G as a direct sum of cyclic groups (at least one of which exists by Theorem II.2.1) yields an isomorphism $G \cong H \oplus F$ where H is a direct sum of finite cyclic groups (possibly $\{0\}$) and F is a free abelian group whose rank is precisely the number s of infinite cyclic summands in the decomposition (see the end of the proof of Theorem II.2.1). We need to show that s is unique and that it does not depend on the decomposition of G.

Theorem II.2.6

Theorem II.2.6. Fundamental Theorem of Finitely Generated Abelian Groups.
Let G be a finitely generated abelian group.

(i) There is a unique nonnegative integer s such that the number of infinite cyclic summands in any decomposition of G as a direct sum of cyclic groups is precisely s.

Proof of (i). Any decomposition of G as a direct sum of cyclic groups (at least one of which exists by Theorem II.2.1) yields an isomorphism $G \cong H \oplus F$ where H is a direct sum of finite cyclic groups (possibly $\{0\}$) and F is a free abelian group whose rank is precisely the number s of infinite cyclic summands in the decomposition (see the end of the proof of Theorem II.2.1). We need to show that s is unique and that it does not depend on the decomposition of G.

Theorem II.2.6 (continued 1)

Proof (continued). If $\iota : H \to H \oplus F$ is the canonical injection $(h \mapsto (h,0))$ then $\iota(H)$ is the torsion subgroup (that is, the subgroup of all elements of finite order) of $H \oplus F$. By Lemma II.2.5(vii), $G_t \cong \iota(H)$ under the isomorphism between G and $H \oplus F$. Of course all subgroups are normal, so by Corollary I.5.8 $G/G_t \cong H \oplus F/\iota(H) \cong F$. So $G/G_t \cong F$, where F is free abelian group of rank s, and this isomorphism is independent of the decomposition $G \cong H \oplus F$. The rank of G/G_t is an invariant by Theorem II.1.2, so this rank s is uniquely determined. □

Theorem II.2.6 (continued 2)

Theorem II.2.6. Fundamental Theorem of Finitely Generated Abelian Groups.
Let G be a finitely generated abelian group.

(iii) Either G is free abelian or there is a list of positive integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_k^{s_k}$ which is unique except for the order of its members, such that $p_1, p_2, \ldots, p_k$ are (not necessarily distinct) primes, $s_1, s_2, \ldots, s_k$ are (not necessarily distinct) positive integers and

$$G \cong \mathbb{Z}_{{p_1}^{s_1}} \oplus \mathbb{Z}_{{p_2}^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{s_k}} \oplus F$$

with F free abelian.

Proof (continued). Suppose G has two decompositions, say $G \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \oplus F$ and $G \cong \sum_{j=1}^{\alpha} \mathbb{Z}_{k_j} \oplus F'$, with each n_i, k_j a power of a prime (the primes may be repeated) and F, F' are free abelian (there is at least one such decomposition by Theorem II.2.).

Theorem II.2.6 (continued 3)

Proof (continued). We must show that (1) $r = d$ and (2) (after reordering) $n_i = k_i$ for every i. The torsion subgroup of $\sum \mathbb{Z}_{n_i} \oplus F$ is isomorphic to $\sum \mathbb{Z}_{n_i}$ and the torsion subgroup of $\sum \mathbb{Z}_{k_j} \oplus F'$ is $\sum \mathbb{Z}_{k_j}$. Hence, $G_t \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j}$. For each prime p,

$$\left(\sum \mathbb{Z}_{n_i}\right)(p) = \left\{ u \in \sum \mathbb{Z}_{n_i} \;\middle|\; \text{the order } |u| = p^n \text{ for some } n \geq 0 \right\}$$

is isomorphic to the direct sum of these $\mathbb{Z}_{n_i}$ such that n_i is a power of p, and similarly $(\sum \mathbb{Z}_{k_j})(p)$ is isomorphic to the direct sum of those $\mathbb{Z}_{k_j}$ such that k_j is a power of p. By Lemma II.2.5(vii), $\left(\sum \mathbb{Z}_{n_i}\right)(p) \cong \left(\sum \mathbb{Z}_{k_j}\right)(p)$ for each power p and by part (i) and Theorem II.1.1(iii) we have that $F \cong F' \cong \sum \mathbb{Z}$ (s summands), so we can assume WLOG that $G = G_t$ and that each n_i, k_j is a power of a fixed prime p (or else we repeat the process for each prime $p_1, p_2, \ldots, p_k$ and then conclude the claimed isomorphism). So we now assume $G = G(p)$.

Theorem II.2.6 (continued 3)

Proof (continued). We must show that (1) $r = d$ and (2) (after reordering) $n_i = k_i$ for every i. The torsion subgroup of $\sum \mathbb{Z}_{n_i} \oplus F$ is isomorphic to $\sum \mathbb{Z}_{n_i}$ and the torsion subgroup of $\sum \mathbb{Z}_{k_j} \oplus F'$ is $\sum \mathbb{Z}_{k_j}$. Hence, $G_t \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j}$. For each prime p,

$$\left(\sum \mathbb{Z}_{n_i}\right)(p) = \left\{ u \in \sum \mathbb{Z}_{n_i} \;\middle|\; \text{the order } |u| = p^n \text{ for some } n \geq 0 \right\}$$

is isomorphic to the direct sum of these $\mathbb{Z}_{n_i}$ such that n_i is a power of p, and similarly $(\sum \mathbb{Z}_{k_j})(p)$ is isomorphic to the direct sum of those $\mathbb{Z}_{k_j}$ such that k_j is a power of p. By Lemma II.2.5(vii), $\left(\sum \mathbb{Z}_{n_i}\right)(p) \cong \left(\sum \mathbb{Z}_{k_j}\right)(p)$ for each power p and by part (i) and Theorem II.1.1(iii) we have that $F \cong F' \cong \sum \mathbb{Z}$ (s summands), so we can assume WLOG that $G = G_t$ and that each n_i, k_j is a power of a fixed prime p (or else we repeat the process for each prime $p_1, p_2, \ldots, p_k$ and then conclude the claimed isomorphism). So we now assume $G = G(p)$.

Theorem II.2.6 (continued 4)

Proof (continued). Hence we have $\sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}} \cong G \cong\cong \sum_{j=1}^{d} \mathbb{Z}_{p^{c_j}}$ where $1 \le a_1 \le a_2 \le \cdots \le a_r$ and $a \le c_1 \le c_2 \le \cdots \le c_d$.

(1) Lemma II.2.5(v) and the decomposition of G using the a_i's gives that $G[p] \cong \sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}}[p] \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (r summands) whence $|G[p]| = p^r$. Similarly, applying this argument to the representation of G using the c_j's give $|G[p]| = p^d$. Therefore $p^r = p^d$ and $r = d$.

Theorem II.2.6 (continued 4)

Proof (continued). Hence we have $\sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}} \cong G \cong\cong \sum_{j=1}^{d} \mathbb{Z}_{p^{c_j}}$ where $1 \le a_1 \le a_2 \le \cdots \le a_r$ and $a \le c_1 \le c_2 \le \cdots \le c_d$.

(1) Lemma II.2.5(v) and the decomposition of G using the a_i's gives that $G[p] \cong \sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}}[p] \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (r summands) whence $|G[p]| = p^r$. Similarly, applying this argument to the representation of G using the c_j's give $|G[p]| = p^d$. Therefore $p^r = p^d$ and $r = d$.

(2) ASSUME there exists v ($1 \le v \le r$) the first integer such that $a_i = c_i$ for all $1 \le i < v$ and $a_n \ne c_v$. We may assume that $a_v < c_v$ (or else we can interchange the a_i's and c_i's). Since

$$\begin{aligned} p^{a_n}\mathbb{Z}_{p^{a_i}} &= \{p^{a_n}u \mid u \in \mathbb{Z}_{p^{a_i}}\} \\ &= \{(p^{a_v - a_i})(p^{a_i}u) \mid u \in \mathbb{Z}_{p^{1_i}}\} \\ &= p^{a_v - a_i}(p^{a_i}\mathbb{Z}_{p^{a_i}}) \\ &\cong p^{a_v - a_i}\mathbb{Z}_{p^{a_i - a_i}} \text{ (by Lemma II.2.5(v))} \cong \{0\} \end{aligned}$$

Theorem II.2.6 (continued 4)

Proof (continued). Hence we have $\sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}} \cong G \cong\cong \sum_{j=1}^{d} \mathbb{Z}_{p^{c_j}}$ where $1 \le a_1 \le a_2 \le \cdots \le a_r$ and $a \le c_1 \le c_2 \le \cdots \le c_d$.

(1) Lemma II.2.5(v) and the decomposition of G using the a_i's gives that $G[p] \cong \sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}}[p] \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (r summands) whence $|G[p]| = p^r$. Similarly, applying this argument to the representation of G using the c_j's give $|G[p]| = p^d$. Therefore $p^r = p^d$ and $r = d$.

(2) ASSUME there exists v $(1 \le v \le r)$ the first integer such that $a_i = c_i$ for all $1 \le i < v$ and $a_n \ne c_v$. We may assume that $a_v < c_v$ (or else we can interchange the a_i's and c_i's). Since

$$\begin{aligned} p^{a_n}\mathbb{Z}_{p^{a_i}} &= \{p^{a_n}u \mid u \in \mathbb{Z}_{p^{a_i}}\} \\ &= \{(p^{a_v - a_i})(p^{a_i}u) \mid u \in \mathbb{Z}_{p^{1_i}}\} \\ &= p^{a_v - a_i}(p^{a_i}\mathbb{Z}_{p^{a_i}}) \\ &\cong p^{a_v - a_i}\mathbb{Z}_{p^{a_i - a_i}} \text{ (by Lemma II.2.5(v))} \cong \{0\} \end{aligned}$$

Theorem II.2.6 (continued 5)

Proof (continued). for all $a_i \leq a_v$, the decomposition of G in terms of the a_i's implies that

$$p^{\alpha_v} G \cong p^{\alpha_v} \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}} \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{a_i - a_v}}$$

(by Lemma II.2.5(v)) with $a_{v+1} - a_v \leq a_{v+2} - a_v \leq \cdots \leq a_r - a_v$. So there are at most $r - v$ nonzero summands. Similarly, since $a_i = c_i$ for $i < v$ and $a_v < c_v$ then the decomposition of G in terms of the c_i's implies that $p^{a_v} G \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{c_i - a_v}}$ with $a \leq c_v - a_v \leq c_{v+1} - a_v \leq \cdots \leq c_r - a_r$. There are at least $r - v + 1$ nonzero summands (since 1 is a lower bound for these parameters). Therefore we have two decompositions of group $p^{a_v} G$ as a direct sum of cyclic groups of prime power order and the number of summands in the first decomposition is strictly less than the number of summands in the second.

Theorem II.2.6 (continued 5)

Proof (continued). for all $a_i \leq a_v$, the decomposition of G in terms of the a_i's implies that

$$p^{\alpha_v} G \cong p^{\alpha_v} \sum_{i=1}^{r} \mathbb{Z}_{p^{\alpha_i}} \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{a_i - a_v}}$$

(by Lemma II.2.5(v)) with $a_{v+1} - a_v \leq a_{v+2} - a_v \leq \cdots \leq a_r - a_v$. So there are at most $r - v$ nonzero summands. Similarly, since $a_i = c_i$ for $i < v$ and $a_v < c_v$ then the decomposition of G in terms of the c_i's implies that $p^{a_v} G \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{c_i - a_v}}$ with $a \leq c_v - a_v \leq c_{v+1} - a_v \leq \cdots \leq c_r - a_r$. There are at least $r - v + 1$ nonzero summands (since 1 is a lower bound for these parameters). Therefore we have two decompositions of group $p^{a_v} G$ as a direct sum of cyclic groups of prime power order and the number of summands in the first decomposition is strictly less than the number of summands in the second.

Theorem II.2.6 (continued 6)

Proof (continued). However, this CONTRADICTS the previous paragraph (part (1)) in which we showed that with the two decompositions (with the a_i's and s_i's) the number of (nonzero) terms are the same ($r = d$); notice that each a_i and c_i is greater than or equal to 1. This contradiction shows that the assumption that such a v exists and so we must have $a_i = c_i$ for all i and hence the representations of G in terms of the a_i's is the same as the representation in terms of the c_i's.

Theorem II.2.6 (continued 7)

Theorem II.2.6. Fundamental Theorem of Finitely Generated Abelian Groups.
Let G be a finitely generated abelian group.

(ii) Either G is free abelian or there is a unique list of (not necessarily distinct) positive integers $m_1, m_2, \ldots, m_t$ such that $m_1 > 1$, $m_1 \mid m_2 \mid \cdots \mid m_t$ and $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F$ with F free abelian.

Proof (continued). (ii) Suppose G has two decompositions, say $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F$ and $G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_{k_d}} \oplus F'$ where $m_1 > 1$, $m_1 \mid m_2 \mid \cdots \mid m_t$ and $k_1 > 1$, $k_1 \mid k_2 \mid \cdots \mid k_d$; and F, F' are free abelian groups. Such a decomposition exists by Theorem II.2.1. We now decompose the m_i's and k_i's into primes and insert factors of the form p^0 so that all parameters are written in terms of the same distinct primes $p_1, p_2, \ldots, p_r$:

Theorem II.2.6 (continued 8)

Proof (continued).

$$\begin{array}{ll} m_1 = p_1^{a_{11}} p_2^{a_{12}} \cdots p_r^{a_{1r}} & k_1 = p_1^{c_{11}} p_2^{c_{12}} \cdots p_r^{c_{1r}} \\ m_2 = p_1^{a_{21}} p_2^{a_{22}} \cdots p_r^{a_{2r}} & k_2 = p_1^{c_{21}} p_2^{c_{22}} \cdots p_r^{c_{2r}} \\ \vdots & \vdots \\ m_t = p_1^{a_{t1}} p_2^{a_{t2}} \cdots p_r^{a_{tr}} & k_d = p_1^{c_{d1}} p_2^{c_{d2}} \cdots p_r^{c_{dr}}. \end{array}$$

Since $m_1 \mid m_2 \mid \cdots \mid m_t$, we must have for each j that $0 \le a_{1j} \le a_{2j} \le \cdots \le a_{tj}$ and similarly for each j that $0 \le c_{1j} \le c_{2j} \le \cdots \le c_{dj}$. We have

$$\begin{aligned} \sum_{i,j} \mathbb{Z}_{p_k^{a_{ij}}} &\cong \sum_{i=1}^{t} \mathbb{Z}_{m_i} \text{ by Lemma II.2.3 since the primes are distinct} \\ &\cong G_t \text{ since these are the elements of finite order,} \\ &\qquad\qquad \text{a group by Lemma II.2.5(iv)} \end{aligned}$$

Theorem II.2.6 (continued 9)

Proof (continued).

$$\begin{aligned}\sum_{i,j} \mathbb{Z}_{p_k^{a_{ij}}} &\cong \mathbb{Z}_{k_i} \\ &\cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}} \text{ by Lemma II.2.3}\end{aligned}$$

where some summands may be 0 (although Lemma II.2.3 is stated for nonzero summands). Since $G(p_j) = \{u \in G \mid |u| = p_j^n \text{ for some } n \geq 0\}$ then for each $j = 1, 2, \ldots, r$ we have

$$\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}} \cong G(p_j) \cong \sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}. \qquad (*)$$

Since $m_1 > 1$, there is some p_j such that $1 \leq a_{1j} \leq a_{2j} \leq \cdots \leq a_{tj}$, whence $\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}}$ has t nonzero summands.

Theorem II.2.6 (continued 10)

Proof (continued). By (iii) $\sum_{i=1}^{d} \mathbb{Z}_{p_j^{c_{ij}}}$ has t nonzero summands as well (since this is another decomposition of $G(p_j)$—it's the $r = d$ part). So $t \leq d$. Similarly, $k_1 > 1$ implies that $d \leq t$ and so $d = t$ and there are the same number of m_i's as k_i's. So we have from $(*)$ that for each j, $\sum_{i=1}^{t} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^{t} \mathbb{Z}_{p_j^{c_{ij}}}$ and by (2) of (iii) we have $a_{ij} = c_{ij}$ for all i. This holds for all j, so $a_{ij} = c_{ij}$ for all i, j. That is $m_i = k_i$ for all i. So the two decompositions are in fact the same and the representation is unique. $\square$