Abstract Algebra I

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

Subsection 1

Direct Products

Direct Products of Groups

Definition (Direct Product)

(1) The direct product $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, G_2, \ldots, G_n$, with operations $\star_1, \star_2, \ldots, \star_n$, respectively, is the set of n-tuples $(g_1, g_2, \ldots, g_n)$, where $g_i \in G_i$, with operation defined componentwise:

$$(g_1, g_2, \ldots, g_n) \star (h_1, h_2, \ldots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \ldots, g_n \star_n h_n).$$

(2) Similarly, the direct product $G_1 \times G_2 \times \cdots$ of the groups $G_1, G_2, \ldots$, with operations $\star_1, \star_2, \ldots$, respectively, is the set of sequences $(g1, g_2, \ldots)$, where $g_i \in G_i$, with operation defined componentwise:

$$(g_1, g_2, \ldots) \star (h_1, h_2, \ldots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \ldots).$$

- The operations may be different in each of the factors, but, as usual, we write all abstract groups multiplicatively:

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

Examples

(1) Suppose $G_i = \mathbb{R}$ (operation addition) for $i = 1, 2, \ldots, n$. Then $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n-factors) is the familiar Euclidean n-space $\mathbb{R}^n$ with usual vector addition:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

(2) The groups forming the direct product may be completely general: Let $G_1 = \mathbb{Z}$, $G_2 = S_3$ and $G_3 = \mathrm{GL}_2(\mathbb{R})$, where the group operations are addition, composition, and matrix multiplication, respectively. Then the operation in $G_1 \times G_2 \times G_3$ is defined by

$$\left(n, \sigma, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\left(m, \tau, \begin{pmatrix} p & q \\ r & s \end{pmatrix}\right) = \left(n + m, \sigma \circ \tau, \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}\right).$$

Products of Groups are Groups

Proposition

If $G_1, \ldots, G_n$ are groups, their direct product is a group of order $|G_1||G_2| \cdots |G_n|$ (if any G_i is infinite, so is the direct product).

- Let $G = G_1 \times G_2 \times \cdots \times G_n$. The group axioms hold for G:
  - **Associative Law**: Let $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ and $(c_1, \ldots, c_n) \in G$. Then
$$\begin{aligned} &(a_1, \ldots, a_n)[(b_1, \ldots, b_n)(c_1, \ldots, c_n)] \\ &= (a_1, \ldots, a_n)(b_1c_1, \ldots, b_nc_n) = (a_1(b_1c_1), \ldots, a_n(b_nc_n)) \\ &= ((a_1b_1)c_1, \ldots, (a_nb_n)c_n) = (a_1b_1, \ldots, a_nb_n)(c_1, \ldots, c_n) \\ &= [(a_1, \ldots, a_n)(b_1, \ldots, b_n)](c_1, \ldots, c_n). \end{aligned}$$
  - The identity of G is the n-tuple $(1_1, 1_2, \ldots, 1_n)$, where 1_i is the identity of G_i.
  - The inverse of $(g_1, g_2, \ldots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$, where g_i^{-1} is the inverse of g_i in G_i.

The formula for the order of G is clear.

Relations Between the Direct Product and its Components

- If the factors of the direct product are rearranged, the resulting direct product is isomorphic to the original one.
- Further, $G_1 \times G_2 \times \cdots \times G_n$ contains an isomorphic copy of each G_i.

Proposition

Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 \times \cdots \times G_n$ their direct product.

(1) For each fixed i, the set of elements of G which have the identity of G_j in the j-th position, for all $j \neq i$, and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i:
$$G_i \cong \{(1, \ldots, 1, g_i, 1, \ldots, 1) : g_i \in G_i\},$$
(here g_i appears in the i-th position). If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(2) For each fixed i, define $\pi_i : G \to G_i$ by $\pi_i((g_1, g_2, \ldots, g_n)) = g_i$. Then π_i is a surjective homomorphism with $\ker\pi_i = \{(g_1, \ldots, g_{i-1}, 1, g_{i+1} \ldots, g_n) : g_j \in G_j,\ \text{for all } j \neq i\} \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(3) Under the identifications in (1), if $x \in G_i$, $y \in G_j$, for $i \neq j$, then $xy = yx$.

Proof of the Proposition

(1) Let $H_i = \{(1, \ldots, 1, g_i, 1, \ldots, 1) : g_i \in G_i\}$.
Claim: H_i is a subgroup of G.
Let $(1, \ldots, 1, g_i, 1, \ldots, 1), (1, \ldots, 1, h_i, 1, \ldots, 1) \in H_i$. Then we have

$$\begin{aligned}&(1, \ldots, 1, g_i, 1, \ldots, 1)(1, \ldots, 1, h_i, 1, \ldots, 1)^{-1} \\ &= (1, \ldots, 1, g_i, 1, \ldots, 1)(1, \ldots, 1, h_i^{-1}, 1, \ldots, 1) \\ &= (1, \ldots, 1, g_i h_i^{-1}, 1, \ldots, 1) \in H_i.\end{aligned}$$

By the subgroup criterion, $H_i \leq G$.
Claim: $G_i \cong H_i$.
Consider $\varphi : G_i \to H_i$, defined by $\varphi(g_i) = (1, 1, \ldots, 1, g_i, 1, \ldots, 1)$.
The map is one-to-one and onto. Further, for all $g_i, h_i \in G_i$,

$$\begin{array}{rcl}\varphi(g_i h_i) & = & (1, \ldots, 1, g_i h_i, 1, \ldots, 1) \\ & = & (1, \ldots, g_i, 1, \ldots, 1)(1, \ldots, 1, h_i, 1, \ldots, 1) \\ & = & \varphi(g_i)\varphi(h_i).\end{array}$$

So φ is an isomorphism and we have $G_i \cong H_i$.

Proof of the Proposition (Cont'd)

- To prove the remaining parts of (1) consider the map $\varphi : G \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ defined by $\varphi(g_1, g_2, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$, i.e., φ erases the i-th component of G. The map φ is a homomorphism since

$$\begin{aligned}
&\varphi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) \\
&= \varphi((g_1 h_1, \cdots, g_n h_n)) \\
&= (g_1 h_1, \ldots, g_{i-1} h_{i-1}, g_{i+1} h_{i+1}, \ldots, g_n h_n) \\
&= (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)(h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n) \\
&= \varphi((g_1, \ldots, g_n))\varphi((h_1, \ldots, h_n)).
\end{aligned}$$

Since the entries in position j are arbitrary elements of G_j, for all j, φ is surjective. Also, $\ker\varphi = \{(g_1, \ldots, g_n) : g_j = 1, \text{for all } j \neq i\} \cong G_i$. Thus, G_i is a normal subgroup of G (in particular, it again proves this copy of G_i is a subgroup). The First Isomorphism Theorem gives $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

Proof of the Proposition (Parts (2) and (3))

(2) $\pi_i : G \to G_i$, with $\pi_i((g_1, \ldots, g_n)) = g_i$ is surjective, since, for all $g_i \in G_i$,
$$\pi_i((1, \ldots, 1, g_i, 1, \ldots, 1)) = g_i.$$
It is a homomorphism, since
$$\begin{array}{rcl} \pi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) & = & \pi_1((g_1 h_1, \ldots, g_n h_n)) \\ & = & g_i h_i \\ & = & \pi_i((g_1, \ldots, g_n))\pi_i((h_1, \ldots, h_n)). \end{array}$$
The kernel of π_i is isomorphic to $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$, via the isomorphism
$$(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) \mapsto (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n).$$

(3) If $x = (1, \ldots, 1, g_i, 1, \ldots, 1)$, $y = (1, \ldots, 1, g_j, 1, \ldots, 1)$, where the indicated entries appear in positions i, j, with, say $i < j$, respectively, then $xy = (1, \ldots, 1, g_i, 1, \ldots, 1, g_j, 1, \ldots, 1) = yx$. This completes the proof.

Components or Factors

- We will identify the "coordinate axis" subgroups

$$H_i = \{(1, \ldots, 1, g_i, 1, \ldots, 1) : g_i \in G_i\}$$

  with their isomorphic copies, the G_i's. The i-th such subgroup is often called the ***i*-th component** or ***i*-th factor** of G.
- Example: When we calculate in $\mathbb{Z}_n \times \mathbb{Z}_m$, we can let x be a generator of the first factor, let y be a generator of the second factor and write the elements of $\mathbb{Z}_n \times \mathbb{Z}_m$ in the form $x^a y^b$.

  This replaces the formal ordered pairs $(x, 1)$ and $(1, y)$, with x and y and, thus, $x^a y^b$ replaces (x^a, y^b).

Examples

(1) By Part (3), if $x_i \in G_i$, $1 \leq i \leq n$, for all $k \in \mathbb{Z}$, $(x_1 x_2 \cdots x_n)^k = x_1^k x_2^k \cdots x_n^k$. The order of $x_1 x_2 \cdots x_n$ is the smallest positive k, such that $x_i^k = 1$, for all i. Hence, $|x_1 x_2 \cdots x_k| = \text{l.c.m.}(|x_1|, |x_2|, \ldots, |x_k|)$, the order being infinite if and only if one of the x_i's has infinite order.

(2) Let p be a prime and for $n \in \mathbb{Z}^+$ consider $E_{p^n} = Z_p \times Z_p \times \cdots \times Z_p$. Then E_{p^n} is abelian of order p^n, such that $x^p = 1$, for all $x \in E_{p^n}$. It is the elementary abelian group of order p^n.

(3) For p a prime, the elementary abelian group of order p^2 has exactly $p+1$ subgroups of order p: Let $E = E_{p^2}$. Each nonidentity element of E has order p, so it generates a cyclic subgroup of E of order p. By Lagrange's Theorem, distinct subgroups of order p intersect trivially. Thus, the $p^2 - 1$ nonidentity elements of E are partitioned into subsets of size $p-1$. So, there are $\frac{p^2-1}{p-1} = p+1$ subgroups of order p. When $p = 2$, E is the Klein 4-group which has 3 subgroups of order 2.

Subsection 2

Recognizing Direct Products

Commutators and Commutator Subgroup

Definition (Commutator Subgroup)

Let G be a group, $x, y \in G$ and A, B be nonempty subsets of G.

(1) Define $[x, y] = x^{-1}y^{-1}xy$, called the **commutator** of x and y.
(2) Define $[A, B] = \langle [a, b] : a \in A, b \in B \rangle$, the group generated by commutators of elements from A and from B.
(3) Define $G' = \langle [x, y] : x, y \in G \rangle$, the subgroup of G generated by commutators of elements from G, called the **commutator subgroup** of G.

- The terminology is due to the fact that:

  The commutator of x and y is 1 if and only if x and y commute.

Properties of Commutators

- Commutators measure the "difference" in G between xy and yx.

Proposition

Let G be a group, $x, y \in G$ and $H \leq G$. Then:

(1) $xy = yx[x, y]$; in particular, $xy = yx$ if and only if $[x, y] = 1$.

(2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.

(3) $\sigma[x, y] = [\sigma(x), \sigma(y)]$, for any automorphism σ of G, G' char G and G/G' is abelian.

(4) G/G' is the largest abelian quotient of G: if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.

(5) If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G', i.e., $G' \leq \ker\varphi$ and the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/G' \arrow[d] \\ & A \end{tikzcd}$$

Proof of the Proposition (Parts (1)-(3))

(1) $xy = yx[x,y]$: $yx[x,y] = yx(x^{-1}y^{-1}xy) = xy$.

(2) $H \trianglelefteq G$ if and only if $[H,G] \leq H$: By definition, $H \trianglelefteq G$ if and only if $g^{-1}hg \in H$, for all $g \in G$, $h \in H$. For $h \in H$, $g^{-1}hg \in H$ if and only if $h^{-1}g^{-1}hg \in H$. So $H \trianglelefteq G$ if and only if $[h,g] \in H$, for all $h \in H$ and all $g \in G$. Thus, $H \trianglelefteq G$ if and only if $[H,G] \leq H$.

(3) $\sigma[x,y] = [\sigma(x),\sigma(y)]$, for $\sigma \in \mathrm{Aut}(G)$, G' char G and G/G' abelian: Let $\sigma \in \mathrm{Aut}(G)$, $x,y \in G$. Then $\sigma([x,y]) = \sigma(x^{-1}y^{-1}xy) = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) = [\sigma(x),\sigma(y)]$. Thus, for every commutator $[x,y]$ of G', $\sigma([x,y])$ is again a commutator. Since σ has a 2-sided inverse, it maps the set of commutators bijectively onto itself. Since the commutators generate G', $\sigma(G') = G'$, i.e., G' char G.

To see that G/G' is abelian, let xG' and yG' be arbitrary elements of G/G'. By definition of the group operation in G/G' and since $[x,y] \in G'$, we have $(xG')(yG') = (xy)G' = (yx[x,y])G' = (yx)G' = (yG')(xG')$.

Proof of the Proposition (Part (4))

(4) G/G' is the largest abelian quotient of G, i.e., if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$: Suppose $H \trianglelefteq G$ and G/H is abelian. Then, for all $x, y \in G$, we have $(xH)(yH) = (yH)(xH)$, so

$$1H = (xH)^{-1}(yH)^{-1}(xH)(yH) = x^{-1}y^{-1}xyH = [x, y]H.$$

Thus $[x, y] \in H$, for all $x, y \in G$, so that $G' \leq H$.

Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian: If $G' \leq H$, then, since, by (3), G/G' is abelian, every subgroup of G/G' is normal. In particular, $H/G' \trianglelefteq G/G'$. By the Lattice Isomorphism Theorem, $H \trianglelefteq G$. By the Third Isomorphism Theorem, $G/H \cong (G/G')/(H/G')$. Hence G/H is abelian.

Proof of the Proposition (Part (5))

(5) Suppose $\varphi : G \to A$ is a homomorphism, with A abelian, and $x, y \in G$. Then

$$\begin{aligned}\varphi([x,y]) &= \varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)\\ &= [\varphi(x),\varphi(y)] = 1.\end{aligned}$$

So, for all $x, y \in G$, $[x, y] \in \ker\varphi$. Thus, $G' \leq \ker\varphi$.
Define $\psi : G/G' \to A$ by $\psi(gG') = \varphi(g)$, for all $g \in G$.

- ψ is well-defined: if $xG' = yG'$, then $y^{-1}x \in G' \leq \ker\varphi$. So $\varphi(y^{-1}x) = 1$, i.e., $\varphi(y)^{-1}\varphi(x) = 1$. So $\varphi(x) = \varphi(y)$.
- ψ is a homomorphism: For all $x, y \in G$,

$$\psi((xG')(yG')) = \psi((xy)G') = \varphi(xy) = \varphi(x)\varphi(y) = \psi(xG')\psi(yG').$$

Finally, the diagram commutes: For all $x \in G$, we get

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/G' \arrow[d, "\psi"] \\ & A \end{tikzcd}$$

$$\psi(\pi(x)) = \psi(xG') = \varphi(x).$$

Some Remarks

- Passing to the quotient by the commutator subgroup of G collapses all commutators to the identity so that all elements in the quotient group commute.
- A strong converse to this also holds:

  A quotient of G by H is abelian if and only if the commutator subgroup is contained in H, i.e., if and only if G' is mapped to the identity in the quotient G/H.
- There are examples of groups with the property that some element in the commutator group cannot be written as a single commutator $[x, y]$, for any $x, y \in G$. Thus, G' does not necessarily consist only of the set of (single) commutators, but is rather the group generated by all the commutators.

Examples (1)-(3)

(1) A group G is abelian if and only if $G' = 1$.

(2) Consider $G = D_8$. We know:

- $Z(D_8) = \langle r^2 \rangle \trianglelefteq D_8$;
- $D_8/Z(D_8)$ is abelian (the Klein 4-group).

Thus, the commutator subgroup D_8' is a subgroup of $Z(D_8)$. Since D_8 is not itself abelian, its commutator subgroup is nontrivial. The only possibility is that $D_8' = Z(D_8)$.

(3) Consider $G = Q_8$. We have:

- $Z(Q_8) = \langle -1 \rangle \trianglelefteq Q_8$;
- $Q_8/Z(Q_8)$ is abelian (the Klein 4-group).

Thus, the commutator subgroup Q_8' is a subgroup of $Z(Q_8)$. Since Q_8 is not itself abelian, its commutator subgroup is nontrivial. The only possibility is that $Q_8' = Z(Q_8) = \langle -1 \rangle$.

Generalizing Examples (2) and (3)

Claim: Let p be prime and G be a nonabelian group of order p^3 with center Z. Then $|Z| = p$, $G/Z \cong Z_p \times Z_p$ and $G' = Z$.

- Since G is a nontrivial group of p-power order, by a previous theorem (using the Class Equation) its center is nontrivial. So $|Z| \neq 1$.
- Since G is nonabelian, $|Z| \neq p^3$.
- Recall that, for any group G, if G/Z is cyclic then G is abelian. So G being nonabelian forces G/Z to be noncyclic. Since a group of prime order is necessarily cyclic, $|G/Z| \neq p$. Hence, $|Z| \neq p^2$.
- The only possibility left is $|Z| = p$.

So $|G/Z| = p^2$. Up to isomorphism the only groups of order p^2 are Z_{p^2} and $Z_p \times Z_p$. Since G/Z is noncyclic, $G/Z \cong Z_p \times Z_p$.

Since G/Z is abelian, we have $G' \subseteq Z$. Because $|Z| = p$ and G' is nontrivial, necessarily $G' = Z$.

Example

Claim: Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1, s^{-1}rs = r^{-1}\rangle$. Then $D'_{2n} = \langle r^2\rangle$.

Since

$$[r, s] = r^{-1}s^{-1}rs = r^{-1}r^{-1}s^{-1}s = r^{-2},$$

we have $\langle r^{-2}\rangle = \langle r^2\rangle \leq D'_{2n}$.

Furthermore, $\langle r^2\rangle \trianglelefteq D_{2n}$ and the images of r and s in $D_{2n}/\langle r^2\rangle$ generate this quotient. Moreover, $r\langle r^2\rangle$ and $s\langle r^2\rangle$ are commuting elements of order ≤ 2. So the quotient is abelian. Thus, $D'_{2n} \leq \langle r^2\rangle$. Therefore, $D'_{2n} = \langle r^2\rangle$.

- If $n(= |r|)$ is odd, $\langle r^2\rangle = \langle r\rangle$;
- If n is even, $\langle r^2\rangle$ is of index 2 in $\langle r\rangle$.

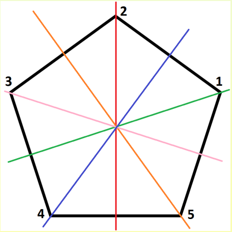
Hence D'_{2n} is of index 2 or 4 in D_{2n} according to whether n is odd or even, respectively.

Commutators and Conjugation

- Conjugation by $g \in G$ is an automorphism of G. So, by Part (3) of the Theorem, $[a^g, b^g] = [a, b]^g$, for all $a, b \in G$. I.e., conjugates of commutators are also commutators.
- It follows that once we exhibit an element of one cycle type in S_n as a commutator, every element of the same cycle type is also a commutator.

  Example: Every 5-cycle is a commutator in S_5.

  Labeling the vertices of a pentagon as $1, \ldots, 5$, we see that $D_{10} \leq S_5$ (a subgroup of A_5 in fact). By the preceding example, an element of order 5 is a commutator in D_{10}, hence also in S_5. Explicitly, $(1\ 4\ 2\ 5\ 3) = [(1\ 2\ 3\ 4\ 5), (2\ 5)(4\ 3)]$.



Expressing Elements in HK

Proposition

Let H and K be subgroups of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, then each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.

- Consider two fixed elements $h_0 \in H$ and $k_0 \in K$. Let
$$S = \{(h,k) \in H \times K : hk = h_0 k_0\}.$$
Define a mapping $\psi : H \cap K \to S$, by setting
$$\psi(\ell) = (h_0\ell, \ell^{-1}k_0), \text{ for all } \ell \in H \cap K.$$
  - ψ is well-defined: Since $\ell \in H \cap K$, we have that $\ell \in H$ and $\ell \in K$. Since $H, K \leq G$, we have $h_0\ell \in H$ and $\ell^{-1}k_0 \in K$. Moreover, we get $(h_0\ell)(\ell^{-1}k_0) = h_0k_0$. Therefore, $\psi(\ell) = (h_0\ell, \ell^{-1}k_0) \in S$.

Expressing Elements in HK (Cont'd)

- ψ is one-one: Suppose $\psi(\ell) = \psi(\ell')$. Then $(h_0\ell, \ell^{-1}k_0) = (h_0\ell', \ell'^{-1}k_0)$. This implies $h_0\ell = h_0\ell'$, whence by cancelation, $\ell = \ell'$.
- ψ is onto: Suppose $(h, k) \in S$. Then $hk = h_0k_0$, whence $h_0^{-1}h = k_0k^{-1} \in H \cap K$. Define $\ell = h_0^{-1}h = k_0k^{-1}$. Then we have

$$\psi(\ell) = (h_0h_0^{-1}h, (k_0k^{-1})^{-1}k_0) = (h, kk_0^{-1}k_0) = (h, k).$$

Thus, ψ is a bijection between S and $H \cap K$. This shows that $|S| = |H \cap K|$, as claimed.

Internal and External Products

Theorem

Suppose G is a group with subgroups H and K, such that:

(1) H and K are normal in G;

(2) $H \cap K = 1$.

Then $HK \cong H \times K$.

- Observe that, by (1), HK is a subgroup of G. Let $h \in H$ and $k \in K$. Since $H \trianglelefteq G$, $k^{-1}hk \in H$, So $h^{-1}(k^{-1}hk) \in H$. Similarly, $(h^{-1}k^{-1}h)k \in K$. Since $H \cap K = 1$, it follows that $h^{-1}k^{-1}hk = 1$, i.e., $hk = kh$. So, every element of H commutes with every element of K. By the preceding proposition, each element of HK can be written uniquely as a product hk, with $h \in H$, $k \in K$. Thus, the map

$$\varphi : HK \to H \times K; \quad hk \mapsto (h,k),$$

is well defined.

Internal and External Products (Cont'd)

- We showed that the map $\varphi : HK \to H \times K$, $hk \mapsto (h, k)$, is well defined. To see that φ is a homomorphism note that if $h_1, h_2 \in H$, $k_1, k_2 \in K$, then h_2 and k_1 commute: $(h_1 k_1)(h_2 k_2) = (h_1 h_2)(k_1 k_2)$. This product is the unique way of writing $(h_1 k_1)(h_2 k_2)$ in the form hk, with $h \in H$ and $k \in K$. This shows that

$$\begin{aligned} \varphi(h_1 k_1 h_2 k_2) &= \varphi(h_1 h_2 k_1 k_2) = (h_1 h_2, k_1 k_2) \\ &= (h_1, k_1)(h_2, k_2) = \varphi(h_1 k_1)\varphi(h_2 k_2). \end{aligned}$$

  The homomorphism φ is a bijection since the representation of each element of HK as a product of the form hk is unique. Thus, φ is an isomorphism.

Internal and External Direct Product

Definition (Internal Direct Product)

If G is a group and H and K are normal subgroups of G, with $H \cap K = 1$, we call HK the **internal direct product** of H and K.
We will call $H \times K$ the **external direct product** of H and K.

- The distinction between internal and external direct product is purely notational: writing elements in the form hk rather than as pairs (h, k).

Example I: For n odd, $D_{4n} \cong D_{2n} \times \mathbb{Z}_2$

(1) If n is a positive odd integer, $D_{4n} \cong D_{2n} \times \mathbb{Z}_2$.

To see this let $D_{4n} = \langle r, s \mid r^{2n} = s^2 = 1, srs = r^{-1} \rangle$ be the usual presentation of D_{4n}. Let $H = \langle s, r^2 \rangle$ and $K = \langle r^n \rangle$. Geometrically, if D_{4n} is the group of symmetries of a regular $2n$-gon, H is the group of symmetries of the regular n-gon inscribed in the $2n$-gon by joining vertex $2i$ to vertex $2i + 2$, for all i mod $2n$ (and if one lets $r_1 = r^2$, H has the usual presentation of the dihedral group of order $2n$ with generators r_1 and s). Note that:

- $H \trianglelefteq D_{4n}$ (it has index 2).
- Since $|r| = 2n$, $|r^n| = 2$. Since $srs = r^{-1}$, we have $sr^n s = r^{-n} = r^n$, i.e., s centralizes r^n. Since clearly r centralizes r^n, $K \leq Z(D_{4n})$. Thus, $K \trianglelefteq D_{4n}$.
- $K \not\leq H$, since r^2 has odd order (or because r^n sends vertex i into vertex $i + n$, hence does not preserve the set of even vertices of the $2n$-gon). Thus, $H \cap K = 1$ by Lagrange.

The preceding theorem now completes the proof.

Example II

(2) Let I be a subset of $\{1, 2, \ldots, n\}$ and let G be the setwise stabilizer of I in S_n , i.e., $G = \{\sigma \in S_n : \sigma(i) \in \mathrm{I}, \text{ for all } i \in \mathrm{I}\}$. Let $\mathrm{J} = \{1, 2, \ldots, n\} - \mathrm{I}$. Note that G is also the setwise stabilizer of J. Let H, K be the pointwise stabilizers of I, J, respectively: Thus, we have

$$H = \{\sigma \in G : \sigma(i) = i \text{ for all } i \in \mathrm{I}\},$$
$$K = \{\tau \in G : \tau(j) = j \text{ for all } j \in \mathrm{J}\}.$$

- It is easy to see that H and K are normal subgroups of G. In fact they are kernels of the actions of G on I and J, respectively.
- Since any element of $H \cap K$ fixes all of $\{1, 2, \ldots, n\}$, we have $H \cap K = 1$.
- Since every element σ of G stabilizes the sets I and J, each cycle in the cycle decomposition of σ involves only elements of I or only elements of J. Thus σ may be written as a product $\sigma_I \sigma_J$, where $\sigma_{\mathrm{I}} \in H$ and $\sigma_{\mathrm{J}} \in K$. This proves $G = HK$.

By the theorem, $G \cong H \times K$.

Example II (Cont'd)

- Any permutation of J can be extended to a permutation in S_n by letting it act as the identity on I. These are precisely the permutations in H. So $H \cong S_{\mathrm{J}}$.
- Similarly the permutations in K are the permutations of I which are the identity on J. So $K \cong S_{\mathrm{I}}$.
- Thus, we get $G \cong S_m \times S_{n-m}$, where $m = |\mathrm{I}|$.

Example III

(3) Let $\sigma \in S_n$ and I be the subset of $\{1, 2, \ldots, n\}$ fixed pointwise by σ: $\mathrm{I} = \{i \in \{1, 2, \ldots, n\} : \sigma(i) = i\}$.

Claim: If $C = C_{S_n}(\sigma)$, then C stabilizes the set I and its complement J.

Let $\tau \in C$ and let $i \in \mathrm{I}$. Then we have

$$\sigma(\tau(i)) = \tau(\sigma(i)) = \tau(i).$$

Thus, $\tau(i) \in \mathrm{I}$, showing that τ stabilizes I. It follows that τ also stabilizes J.

By the preceding example, C is isomorphic to a subgroup of $H \times K$, where H is the subgroup of all permutations in S_n fixing I pointwise and K is the set of all permutations fixing J pointwise. Note that $\sigma \in H$. Thus each element α of C can be written (uniquely) as $\alpha = \alpha_{\mathrm{I}}\alpha_{\mathrm{J}}$, for some $a_{\mathrm{I}} \in H$ and $\alpha_{\mathrm{J}} \in K$.

Example III (Cont'd)

- If τ is any permutation of $\{1, 2, \ldots, n\}$, which fixes each $j \in \mathrm{J}$, i.e., any element of K, then σ and τ commute (since they move no common integers). Thus, C contains all such τ, i.e., C contains the subgroup K. This proves that the group C consists of all elements $\alpha_{\mathrm{I}}\alpha_{\mathrm{J}} \in H \times K$, such that α_{J} is arbitrary in K and α_{I} commutes with σ in H:

$$C_{S_n}(\sigma) = C_H(\sigma) \times K \cong C_{S_{\mathrm{J}}}(\sigma) \times S_{\mathrm{I}}.$$

In particular, if σ is an m-cycle in S_n, $C_{S_n}(\sigma) = \langle \sigma \rangle \times S_{n-m}$.

The latter group has order $m(n-m)!$.

Subsection 3

The Fundamental Theorem of Finitely Generated Abelian Groups

Finitely Generated and Free Abelian Groups

Definition (Finitely Generated and Free Abelian Groups)

(1) A group G is **finitely generated** if there is a finite subset A of G, such that $G = \langle A \rangle$.

(2) For each $r \in \mathbb{Z}$, with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the **free abelian group of rank r**.

- Any finite group G is, a fortiori, finitely generated, since we may simply take $A = G$ as a set of generators.
- Also, $\mathbb{Z}^r$ is finitely generated by $e_1, e_2, \ldots, e_n$, where

$$e_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$$

is the n-tuple with 1 in position i and zeros elsewhere.

The Fundamental Theorem of Finitely Generated Abelian Groups

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

Let G be a finitely generated abelian group. Then:

(1) $G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$, for some integers r, n_1, n_2, ..., n_s satisfying the following conditions:
  (a) $r \geq 0$ and $n_j \geq 2$, for all j;
  (b) $n_{i+1} \mid n_i$, for $1 \leq i \leq s-1$.

(2) The expression in (1) is unique: if

$$G \cong \mathbb{Z}^t \times Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_u}.$$

where t and m_1, m_2, ..., m_u satisfy (a) and (b), i.e., $t \geq 0$, $m_j \geq 2$, for all j, and $m_{i+1} \mid m_i$, for $1 \leq i \leq u-1$, then $t = r$, $u = s$ and $m_i = n_i$, for all i.

- The proof of the Fundamental Theorem is in Abstract Algebra II.

Free Rank and Invariant Factor Decomposition

Definition (Free Rank and Invariant Factor Decomposition)

The integer r in the expression $G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$ is called the **free rank** or **Betti number** of G. The integers n_1, n_2, …, n_s are called the **invariant factors** of G. The description itself is called the **invariant factor decomposition** of G.

- The Fundamental Theorem asserts that the free rank and (ordered) list of invariant factors of an abelian group are uniquely determined.
- Thus, two finitely generated abelian groups are isomorphic if and only if they have the same free rank and the same list of invariant factors.
- A finitely generated abelian group is a finite group if and only if its free rank is zero. In that case, the order is just the product of its invariant factors.
- If G is a finite abelian group with invariant factors n_1, n_2, …, n_s, where $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$, then G is **of type** $(n_1, n_2, \ldots, n_s)$.

Isomorphism Classes and Types

- The Fundamental Theorem gives an effective way of listing all finite abelian groups of a given order:

  To find (up to isomorphism) all abelian groups of a given order n, we must find all finite sequences of integers n_1, n_2, ..., n_s, such that
  (1) $n_j \geq 2$, for all $j \in \{1, 2, \ldots, s\}$;
  (2) $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$;
  (3) $n_1 n_2 \cdots n_s = n$.
- The Theorem asserts that there is a bijection between the set of such sequences and the set of isomorphism classes of finite abelian groups of order n.

  Under the bijection, each sequence corresponds to the list of invariant factors of a finite abelian group.

Some Remarks on the Invariant Factor Decomposition

- Consider, again, the invariant factor decomposition of a finite abelian group G of order n:
$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$
The following remarks apply:
  - $n_1 \geq n_2 \geq \cdots \geq n_s$, so n_1 is the largest invariant factor.
  - Each n_i divides n.
  - If p is any prime divisor of n, then p must divide n_i, for some i. Then p also divides n_j, for all $j \leq i$. It follows that every prime divisor of n must divide the first invariant factor n_1.

Corollary

If n is the product of distinct primes, then, up to isomorphism, the only abelian group of order n is the cyclic group Z_n of order n.

- If n is the product of distinct primes, $n \mid n_1$. Hence $n = n_1$. Thus, if n is square free, there is only one possible list of invariant factors for an abelian group of order n, namely, the list $n_1 = n$.

Abelian Groups of Order 180

- Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$. We must have $2 \cdot 3 \cdot 5 \mid n_1$. So possible values of n_1 are
$$n_1 = 2^2 \cdot 3^2 \cdot 5, \quad 2^2 \cdot 3 \cdot 5, \quad 2 \cdot 3^2 \cdot 5, \quad 2 \cdot 3 \cdot 5.$$
For each of these, one must work out all possible n_2's (subject to $n_2 \mid n_1$ and $n_1 n_2 \mid n$). For each resulting pair n_1, n_2 one must work out all possible n_3's etc. until all lists satisfying (1) to (3) are obtained.
- If $n_1 = 2 \cdot 3^2 \cdot 5$, the only number n_2 dividing n_1, with $n_1 n_2$ dividing n, is $n_2 = 2$. In this case $n_1 n_2 = n$. So this list is complete: $2 \cdot 3^2 \cdot 5, 2$. The abelian group corresponding to this list is $Z_{90} \times Z_2$.
- If $n_1 = 2 \cdot 3 \cdot 5$, the only candidates for n_2 are $n_2 = 2, 3$ or 6. If $n_2 = 2$ or 3, then since $n_3 \mid n_2$, we would necessarily have $n_3 = n_2$. This is not possible since n is not divisible 2^3 or 3^3. Thus, the only list of invariant factors whose first term is $2 \cdot 3 \cdot 5$ is $2 \cdot 3 \cdot 5, 2 \cdot 3$. The corresponding abelian group is $Z_{30} \times Z_6$.
- The complete list of isomorphism types is $Z_{180}, Z_{90} \times Z_2, Z_{60} \times Z_3$ and $Z_{30} \times Z_6$.

The Primary Decomposition Theorem

Theorem (The Primary Decomposition Theorem)

Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Then:

(1) $G \cong A_1 \times A_2 \times \cdots \times A_k$. where $|A_i| = p_i^{\alpha_i}$.

(2) For each $A \in \{A_1, A_2, \ldots, A_k\}$, with $|A| = p^\alpha$, $A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$, with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ (t and $\beta_1, \ldots, \beta_t$ depend on i).

(3) The decomposition in (1) and (2) is unique, i.e., if $G \cong B_1 \times B_2 \times \cdots \times B_m$, with $|B_i| = p_i^{\alpha_i}$, for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Definition

The integers p^{β_j}, described in the preceding theorem, are called the **elementary divisors** of G. The description of G in the theorem is called the **elementary divisor decomposition** of G.

Remarks on the Primary Decomposition Theorem

- The subgroups A_i described in Part (1) of the theorem are the Sylow p_i-subgroups of G.
- Thus (1) says that G is isomorphic to the direct product of its Sylow subgroups (they are normal, since G is abelian and, hence, unique).
- For p a prime, $p^\beta \mid p^\gamma$ if and only if $\beta \leq \gamma$. Furthermore, $p^{\beta_1} \cdots p^{\beta_t} = p^\alpha$ if and only if $\beta_1 + \cdots + \beta_t = \alpha$.

  Thus, the decomposition of A appearing in Part (2) of the theorem is the invariant factor decomposition of A with the "divisibility" conditions on the integers p^{β_j} translated into "additive" conditions on their exponents.

  The elementary divisors of G are now seen to be the invariant factors of the Sylow p-subgroups as p runs over all prime divisors of G.

Invariant Factors of Primary Components

- In order to find all abelian groups of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, one must find for each i, $1 \leq i \leq k$, all possible lists of invariant factors for groups of order $p_i^{\alpha_i}$.
- The set of elementary divisors of each abelian group is then obtained by taking one set of invariant factors from each of the k lists.
- The abelian groups are the direct products of the cyclic groups whose orders are the elementary divisors (and distinct lists of elementary divisors give non isomorphic groups).
- We must obey the following conditions for the invariant factors:
  (1) $\beta_j \geq 1$, for all $j \in \{1, 2, \ldots, t\}$;
  (2) $\beta_i \geq \beta_{i+1}$, for all i;
  (3) $\beta_1 + \beta_2 + \cdots + \beta_t = \beta$.

Abelian Groups of Order p^5

- The number of nonisomorphic abelian groups of order p^β equals the number of partitions of β, which is independent of the prime p.

  Example: The number of abelian groups of order p^5 is obtained from the list of partitions of 5:

Partitions of 5	Abelian Groups
5	Z_{p^5}
$4, 1$	$Z_{p^4} \times Z_p$
$3, 2$	$Z_{p^3} \times Z_{p^2}$
$3, 1, 1$	$Z_{p^3} \times Z_p \times Z_p$
$2, 2, 1$	$Z_{p^2} \times Z_{p^2} \times Z_p$
$2, 1, 1, 1$	$Z_{p^2} \times Z_p \times Z_p \times Z_p$
$1, 1, 1, 1, 1$	$Z_p \times Z_p \times Z_p \times Z_p \times Z_p$

  Thus there are precisely 7 non isomorphic groups of order p^5.
  - The first in the list is the cyclic group Z_{p^5}.
  - The last in the list is the elementary abelian group E_{p^5}.

Abelian Groups of Order 1800

- If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and q_i is the number of partitions of α_i, we see that the number of (distinct, non isomorphic) abelian groups of order n equals $q_1 q_2 \cdots q_k$.
- Example: If $n = 1800 = 2^3 3^2 5^2$ we list the abelian groups of this order as follows:

Order p^β	Partitions of β	Abelian Groups
2^3	$3; 2, 1; 1, 1, 1$	$Z_8, Z_4 \times Z_2, Z_2 \times Z_2 \times Z_2$
3^2	$2; 1, 1$	$Z_9, Z_3 \times Z_3$
5^2	$2; 1, 1$	$Z_{25}, Z_5 \times Z_5$

  The abelian groups of order 1800 are obtained by taking one abelian group from each of the three lists and taking their direct product: This results in $3 \times 2 \times 2 = 12$ abelian groups of order 1800.
- It is important to keep in mind that the elementary divisors of G are not invariant factors of G, but invariant factors of subgroups of G.

A Decomposition Theorem

Proposition

Let $m, n \in \mathbb{Z}^+$.

(1) $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.

(2) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

(1) Let $Z_m = \langle x \rangle$, $Z_n = \langle y \rangle$ and let $\ell = \text{l.c.m.}(m, n)$. Note that $\ell = mn$ if and only if $(m, n) = 1$. Let $x^a y^b$ be a typical element of $Z_m \times Z_n$. Then $(x^a y^b)^\ell = x^{\ell a} y^{\ell b} = 1^a 1^b = 1$.

- If $(m, n) \neq 1$, every element of $Z_m \times Z_n$ has order at most ℓ. So it has order strictly less than mn. Thus, $Z_m \times Z_n$ cannot be isomorphic to Z_{mn}.
- Conversely, if $(m, n) = 1$, then $|xy| = \text{l.c.m.}(|x|, |y|) = mn$. Thus, by order considerations, $Z_m \times Z_n = \langle xy \rangle$ is cyclic, completing the proof.

A Decomposition Theorem (Part (2))

(2) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. We show that $Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}}$ by induction on k.

For $k = 1$ this is trivial.

For $k = 2$, we have

$$Z_n = Z_{p_1^{\alpha_1} p_2^{\alpha_2}} \stackrel{\text{Part (1)}}{\cong} Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}}.$$

Suppose the result holds for some $k \geq 2$.

Then, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}$, we get

$$\begin{aligned} Z_n \cong Z_{p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}} & \stackrel{\text{Part (1)}}{\cong} Z_{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \times Z_{p_{k+1}^{\alpha_{k+1}}} \\ & \stackrel{\text{Ind.Hyp.}}{\cong} Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}} \times Z_{p_{k+1}^{\alpha_{k+1}}}. \end{aligned}$$

From Invariant Factors to Elementary Divisors

- Suppose G is given as an abelian group of type $(n_1, n_2, \ldots, n_s)$, i.e.,

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n_1 n_2 \cdots n_s$. Factor each n_i as

$$n_i = p_1^{\beta_{i1}} p_2^{\beta_{i2}} \cdots p_k^{\beta_{ik}},$$

where $\beta_{ij} \geq 0$. By the proposition,

$$Z_{n_i} \cong Z_{p_1^{\beta_{i1}}} \times Z_{p_2^{\beta_{i2}}} \times \cdots \times Z_{p_k^{\beta_{ik}}},$$

for each i. If $\beta_{ij} = 0$, $Z_{p_j^{\beta_{ij}}} = 1$ and this factor may be deleted from the direct product. Then the elementary divisors of G are precisely the integers

$$p_j^{\beta_{ij}},\ 1 \leq j \leq k,\ 1 \leq i \leq s,\ \text{such that } \beta_{ij} \neq 0.$$

Example: Invariant Factors to Elementary Divisors

- If $|G| = 2^3 \cdot 3^2 \cdot 5^2$ and G is of type $(30, 30, 2)$, then
$$G \cong Z_{30} \times Z_{30} \times Z_2.$$
Since $Z_{30} \cong Z_2 \times Z_3 \times Z_5$,
$$G \cong Z_2 \times Z_3 \times Z_5 \times Z_2 \times Z_3 \times Z_5 \times Z_2.$$
The elementary divisors of G are $2, 3, 5, 2, 3, 5, 2$, or, grouping like primes together, $2, 2, 2, 3, 3, 5, 5$.
If for each j, the factors $Z_{p_j^{\beta_{ij}}}$ are put together, the resulting direct product forms the Sylow p_j-subgroup A_j of G.
Thus, the Sylow 2-subgroup of the group above is
$$\cong Z_2 \times Z_2 \times Z_2.$$

From Cyclic Decompositions to Elementary Divisors

- This same process will give the elementary divisors of a finite abelian group G whenever G is given as a direct product of cyclic groups (not just when the orders of the cyclic components are the invariant factors).
- Example: If $G = Z_6 \times Z_{15}$, the list 6, 15 is
  - neither that of the invariant factors (the divisibility condition fails)
  - nor that of elementary divisors (they are not prime powers).

  To find the elementary divisors, factor $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$. Then the prime powers 2, 3, 3, 5 are the elementary divisors and

$$G \cong Z_2 \times Z_3 \times Z_3 \times Z_5.$$

From Elementary Divisors to Invariant Factors

- Suppose G is an abelian group of order n, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and we are given the elementary divisors of G.

  The invariant factors of G are obtained as follows:

  (1) First group all elementary divisors which are powers of the same prime together.
  In this way we obtain k lists of integers (one for each p_k).

  (2) In each of these k lists arrange the integers in non-increasing order.

  (3) Among these k lists suppose that the longest, i.e., the one with the most terms, consists of t integers.
  Make each of the k lists of length t by appending an appropriate number of 1's at the end of each list.

  (4) For each $i \in \{1, 2, \ldots, t\}$ the i-th invariant factor, n_i, is obtained by taking the product of the i-th integer in each of the t (ordered) lists.

- The point of ordering the lists in this way is to ensure that we have the divisibility condition $n_{i+1} \mid n_i$.

Obtaining Invariant Factors From Elementary Divisors

- Suppose that the elementary divisors of G are given as $2, 3, 2, 25, 3, 2$ (so $|G| = 2^3 \cdot 3^2 \cdot 25$).

  Regrouping and increasing each list to have 3 ($= t$) members gives:

$p = 2$	2	2	2
$p = 3$	3	3	1
$p = 5$	25	1	1

  So the invariant factors of G are

  $$2 \cdot 3 \cdot 25, \quad 2 \cdot 3 \cdot 1, \quad 2 \cdot 1 \cdot 1.$$

  and

  $$G \cong Z_{150} \times Z_6 \times Z_2.$$

Using Elementary Divisors to Check Isomorphism

- We can use the decompositions to determine whether any two direct products of finite cyclic groups are isomorphic.

  Example: We want to determine whether $Z_6 \times Z_{15} \cong Z_{10} \times Z_9$.
  - First determine whether they have the same order (both have order 90).
  - Then (the easiest way in general) determine whether they have the same elementary divisors:
    - $Z_6 \times Z_{15}$ has elementary divisors 2, 3, 3, 5. It is isomorphic to $Z_2 \times Z_3 \times Z_3 \times Z_5$.
    - $Z_{10} \times Z_9$ has elementary divisors 2, 5, 9. It is isomorphic to $Z_2 \times Z_5 \times Z_9$.

  The lists of elementary divisors are different so the groups are not isomorphic.