Supplementary Notes on Direct Products of Groups and the Fundamental Theorem of Finite Abelian Groups

Definition. Let $G_1, G_2, \ldots G_n$ be groups. We can make the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ into a group via coordinate-wise multiplication:

$$(g_1, g_2, \ldots, g_n) \cdot (g_1', g_2', \ldots, g_n') = (g_1g_1', g_2g_2', \ldots, g_ng_n').$$

It is absolutely routine to check that with the above operation, $G_1 \times G_2 \times \cdots \times G_n$ is a group, called the *(external) direct product* of $G_1, G_2, \ldots G_n$.

In case $G_1, G_2, \ldots, G_n$ are abelian groups written additively, then it is more customary to write the direct product as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, and refer to this as an *(external) direct sum.*

To "internalize" this notion, recall first that if G is a group with *normal* subgroups $H, K \triangleleft G$, then the product HK is a subgroup of G. More generally, if we have normal subgroups $H_1, H_2, \ldots, H_n \triangleleft G$, then the product $H_1H_2\cdots H_n$ is also a subgroup of G. Sometimes this represents G as a direct product, as follows:

Theorem 1. [Internal Direct Product Theorem] *Let $H_1, H_2, \ldots, H_n$ be normal subgroups of G, and assume that*

(i) $G = H_1H_2\cdots H_n$,

(ii) For each $i = 1, 2, \ldots, n$, we have $H_i \cap (H_1 \cdots H_{i-1}H_{i+1}\cdots H_n) = \{e\}$.

Then $G \cong H_1 \times H_2 \times \cdots \times H_n$; in fact the mapping

$$\phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow G$$

given by $\phi(h_1, h_2, \ldots, h_n) = h_1h_2\cdots h_n$ is an isomorphism. When this happens, we shall slur the distinction between "internal" and "external" and simply write $G = H_1 \times H_2 \times \cdots \times H_n$, keeping in mind that H_1, H_2, $\ldots$, H_n are actually subgroups *of G.*

Proof. We claim first that if $h_i \in H_i$ and $h_j \in H_j$ with $i \neq j$, then $h_ih_j = h_jh_i$. But this is easy: since both H_i and H_j are normal in G, we see that the "commutator" $h_ih_jh_i^{-1}h_j^{-1} \in H_i \cap H_j$. But condition (ii) above clearly implies that $H_i \cap H_j = \{e\}$, and so it follows that $h_ih_j = h_jh_i$, as required. Now define

$$\phi : H_1 \times H_2 \times \cdots \times H_n \longrightarrow G$$

by setting $\phi(h_1, h_2, \ldots, h_n) = h_1h_2\cdots h_n$. Because of what we just proved above, ϕ is a homomorphism. By condition (i), ϕ is onto. Finally, if $(h_1, h_2, \ldots, h_n) \in \ker\,\phi$, then $h_1h_2\cdots h_n = e$ implies that $h_i^{-1} = h_1\cdots h_{i-1}h_{i+1}\cdots h_n \in H_i \cap (H_1\cdots H_{i-1}H_{i+1}\cdots H_n) = \{e\}$, i.e., $h_i = e$. Since i was arbitrary, we conclude that $(h_1, h_2, \ldots, h_n) = (e, e, \ldots, e)$, and so ϕ is also injective. This proves the theorem.

Please note that for abelian groups written additively, there is an obvious analogue of the above result.

We shall now turn our attention to finite abelian groups. Basically we shall try to prove that every finite abelian group can be decomposed into cyclic groups. Without further stipulations, we can't really hope for a uniqueness result, basically because of the

Theorem 2. [Chinese Remainder Theorem] *Let m and n be relatively prime integers and let $Z_m,\ Z_n,\ Z_{mn}$ be cyclic groups of the given orders. Then $Z_m \times Z_n \cong Z_{mn}$.*

Proof. Let Z_{mn} be generated by the element z. Then the elements $z_1 = z^n,\ z_2 = z^m$ have orders m and n, respectively. Set $H_1 = \langle z_1\rangle,\ H_2 = \langle z_2\rangle$ (cyclic groups of orders m and n, respectively), and note that the hypotheses of the above theorem are met, i.e., $Z_{mn} \cong H_1 \times H_2$.

Notice that the Chinese Remainder Theorem allows us to consolidate many direct product decompositions of cyclic groups into fewer such products, or to reconfigure direct products, as the following examples indicate:

$Z_6 \times Z_7 \cong Z_{42}$,

$Z_2 \times Z_5 \times Z_7 \cong Z_{70}$,

$Z_6 \times Z_{35} \cong Z_2 \times Z_3 \times Z_{35} \cong Z_2 \times Z_{105}$.

Now let A be a finite abelian group, which we continue to write multiplicatively. Let $|A| = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ be the decomposition of the order of A into distinct prime factors. We set $n = |A|$, and set

$$n_1 = \frac{n}{p_1^{a_1}},\ n_2 = \frac{n}{p_2^{a_2}},\ \ldots, n_k = \frac{n}{p_k^{a_k}}.$$

Note that while the integers $n_1, n_2, \ldots, n_k$ are not pairwise relatively prime, they are *collectively* relatively prime, meaning that there is no integer greater than 1 than divides all of them. This implies, since $\mathbb{Z}$ is a principal ideal domain, that the ideal $(n_1, n_2, \ldots, n_k) = (1) = \mathbb{Z}$, which further implies that there exist integers $s_1, s_2, \ldots, s_k \in \mathbb{Z}$, with $s_1n_1 + s_2n_s + \cdots s_kn_k = 1$.

Using the above, we can prove the following fundamental result.

Theorem 3. [Primary Decomposition Theorem] *Let A be a finite abelian group of order $|A| = n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, and let P_i be the p_i-Sylow subgroup of A, $i = 1, 2, \ldots, k$. Then $A = P_1 \times P_2 \times \cdots \times P_k$.*

Proof. We shall show that the hypotheses of *Theorem* 1 are satisfied. Note first that since A is abelian, then every subgroup of A is normal. In particular, the Sylow subgroups $P_1,\ P_2,\ \ldots,\ P_k$ are all normal. Furthermore, if $a \in A$ is an element whose order is a power of p_i, then it follows from Sylow's Theorem (the "covering" part) that a is contained in a p_i-Sylow subgroup. But there is only *one* p_i-Sylow subgroup since all are conjugate and any one is normal. Therefore, it follows that $a \in P_i$.

Next, let $a \in A$ be an arbitrary element. Using the result above, we have $s_1n_1 + s_2n_s + \cdots s_kn_k = 1$, for suitable $s_1,\ s_2,\ \ldots,\ s_k \in \mathbb{Z}$, and so

$$a \;=\; a^1 \;=\; a^{s_1n_1+s_2n_s+\cdots s_kn_k} = a^{s_1n_1}a^{s_2n_2}\cdots a^{s_kn_k}.$$

However, $(a^{s_in_i})^{p_i^{a_i}} = (a^n)^{s_i} = e^{s_i} = e$ and so $a^{s_in_i} \in P_i$, for $i = 1, 2, \ldots, k$. This already proves that $A = P_1P_2\cdots P_k$. That $P_i \cap (P_1 \cdots P_{i-1}P_{i+1}\cdots P_k) = \{e\}$ should be obvious. This proves the theorem.

At this stage, we see that the decomposition of a finite abelian group into a direct product of cyclic groups can be accomplished once we show that any abelian p-group can be factored into a direct product of cyclic p-groups.

Theorem 4. *Let P be a finite abelian p-group of order p^m. Then there exist powers $e_1, e_2, \ldots, e_r$ with $e_1 \geq e_2 \geq \cdots \geq e_r$ such that $P \cong Z_{p^{e_1}} \times Z_{p^{e_2}} \times \cdots \times Z_{p^{e_r}}$.*

Proof. We shall argue by induction on the order of P. First, let $x_1 \in P$ be an element of maximal order p^{e_1} in P. Clearly, $e_1 \leq m$. Set $Z_1 = \langle x_1\rangle$. By induction, the quotient group A/Z_1 is a direct product of cyclic groups:

$$A/Z_1 \;=\; \langle y_2Z_1\rangle \times \langle y_3Z_1\rangle \times \cdots \times \langle y_rZ_1\rangle,$$

where $o(y_2Z_1) = p^{e_2}, \ldots, o(y_rZ_1) = p^{e_r},\ e_2 \geq e_3 \geq \cdots \geq e_r$. Note that since x_1 has maximal order in A, it follows that $e_1 \geq e_2$.

Now we shall make some adjustments. Fix i, where $2 \leq i \leq r$, and consider the cyclic subgroup $\langle y_iZ_1\rangle \leq A/Z_1$. Since $o(y_iZ_1) = p^{e_i}$ we have $y_i^{p^{e_i}} \in Z_1$, say $y_i^{p^{e_i}} = x_1^{k_i}$. Thus $(x_1^{k_i})^{p^{e_1-e_i}} = (y_i^{p^{e_i}})^{p^{e_1-e_i}} = y_i^{p^{e_1}} = e$ and so $p^{e_1}|k_ip^{e_1-e_i}$. Thus $p^{e_i}|k_i$, say $k_i = l_ip^{e_i}$, so $y_i^{p^{e_i}} = x_1^{k_i} = x_1^{l_ip^{e_i}}$. Now the adjustment: we set $x_i = y_ix_1^{-l_i}$, so $x_i^{p^{e_i}} = y_i^{p^{e_i}}x_1^{-l_ip^{e_i}} = e$, and *no smaller exponent kills* x_i. Doing this for each

$i = 2, 3, \ldots, r$ produces elements $x_2, x_3, \ldots, x_r \in P$ such that $o(x_i) = p^{e_i}$, $i = 2, 3, \ldots, r$. Set $Z_2 = \langle x_2 \rangle$, $Z_3 = \langle x_3 \rangle, \ldots, Z_r = \langle x_r \rangle$. To finish the proof, we need to show:

(i) $P = Z_1 Z_2 \cdots Z_r$,

(ii) $Z_i \cap (Z_1 \cdots Z_{i-1} Z_{i+1} \cdots Z_r) = \{e\}$.

Let $x \in P$. From the product decomposition above for A/Z_1, we have powers $f_2, f_3, \ldots, f_r$ with

$$(y_2 Z_1)^{f_2} (y_3 Z_1)^{f_3} \cdots (y_r Z_1)^{f_r} \ = \ x Z_1,$$

so it follows that $y_2^{f_2} \cdots y_r^{f_r} = x x'$, for some $x' \in Z_1$. Thus, since $y_i = x_i x_1^{l_i}$, we get

$$x_2^{f_2} x_3^{f_3} \cdots x_r^{f_r} \ = \ x x'',$$

for some $x'' \in Z_1$. Now let f_1 be such that $x_1^{f_1} = (x'')^{-1}$, and conclude that $x_1^{f_1} x_2^{f_2} \cdots x_r^{f_r} = x$, proving part (i).

To prove part (ii), note that it suffices to prove that if

$$x_1^{f_1} x_2^{f_2} \cdots x_r^{f_r} \ = \ e,$$

then $p^{e_i} | f_i$, for $i = 1, 2, \ldots, r$. Again, since $x_i = y_i x_1^{-l_i}$, $i = 2, 3, \ldots, r$ we get an equation of the form

$$x' y_2^{f_2} y_3^{f_3} \cdots y_r^{f_r} \ = \ e,$$

for some $x' \in Z_1$, from which we conclude that

$$(y_2 Z_1)^{f_2} (y_3 Z_1)^{f_3} \cdots (y_r Z_1)^{f_r} \ = \ e Z_1;$$

this implies that $p^{e_i} | f_i$, $i = 2, 3, \ldots, r$. But then it follows immediately that $x_1^{f_1} = e$, and so $p^{e_1} | f_1$, as well. This completes the proof.

If we use the above theorem, together with the Chinese Remainder Theorem, we get the following ”existence” theorem.

Theorem 5. [Existence of Invariant Factors] *Let A be a finite abelian group, and let $n = |A|$ be the order of A. Then there exists a decreasing sequence $n_1 \geq n_2 \geq \cdots \geq n_s$, with $n_s | n_{s-1}$, $n_{s-1} | n_{s-2}, \ldots, n_2 | n_1$, and cyclic subgroups Z_1, $Z_2, \ldots, Z_s$ of orders $n_1, n_2, \ldots, n_s$, respectively with $A = Z_1 \times Z_2 \times \cdots \times Z_s$. The numbers n_1, n_2, $\ldots$, n_s are called* invariant factors *of A.*

It is pretty easy to see how the direct product decompositions of the Sylow subgroups in the Primary Decomposition Theorem can be synthesized into a direct product decomposition of the type indicated above. For example, if we had a group $A = P_1 \times P_2 \times P_3 \times P_4$, (direct decomposition into Sylow subgroups), with $P_1 \cong Z_8 \times Z_4$, $P_2 \cong Z_9 \times Z_3$, $P_3 \cong Z_{125} \times Z_5 \times Z_5 \times Z_5$, and $P_4 \cong Z_{11}$, (note here that I've written Z_n for a cyclic group of order n; sorry about being somewhat inconsistent in my usage), then we would have

$$A \cong Z_8 \times Z_4 \times Z_9 \times Z_3 \times Z_{125} \times Z_5 \times Z_5 \times Z_5 \times Z_{11},$$

and so a reorganized direct product decomposition would look like:

$$A \cong Z_{8 \cdot 9 \cdot 125 \cdot 11} \times Z_{4 \cdot 3 \cdot 5} \times Z_5 \times Z_5,$$

and so the "invariant factors" are $n_1 = 8 \cdot 9 \cdot 125 \cdot 11 = 99,000,\ n_2 = 4 \cdot 3 \cdot 5 = 60,\ n_3 = 5,\ n_4 = 5$.

To obtain a uniqueness result for the direct product decomposition, we shall first discuss the question of "cancellation" in a direct product decomposition. Basically, the question is this: If we have an isomorphism of direct product groups,

$$G_1 \ \times \ H_1 \ \cong G_2 \ \times \ H_2,$$

with $H_1 \cong H_2$, is it true that $G_1 \cong G_2$? The naive student will quickly respond with an affirmative answer; yet the answer is no, making the cancellation question rather subtle. As a counterexample to the cancellation problem, consider the infinite direct product of the infinite cyclic group Z:

$$Z \times (Z \times \cdots) \ \cong \ Z \times Z \times (Z \times \cdots);$$

note that if we could cancel off the right hand factors, when we would end up with $Z \cong Z \times Z$, which is false (Z is cyclic, but $Z \times Z$ is not). Therefore we must treat this question with some care.

Before turning to the main cancellation result, let's state and prove a very simple lemma, and recall another important result.

Lemma. *Suppose we have groups and normal subgroups: $M \triangleleft A,\ N \triangleleft B$. Then $M \times N \triangleleft A \times B$, and*

$$(A \times B)/(M \times N) \ \cong \ (A/M) \times (B/N).$$

Proof. Clearly the first statement above is true. As for the isomorphism, define $\phi : A \times B \to (A/M) \times (B/N)$, by setting $\phi(a, b) = (aM, bN)$. Note that ϕ is a surjective homomorphism with kernel $M \times N$.

Theorem 6. [Noether Isomorphism Theorem] *Let G be a group and let $H, K \leq G$, with $K \triangleleft G$. Then*

$$HK/K \;\cong\; H/(H \cap K).$$

In particular, if we have $H, K \triangleleft G$ and $H \cap K = \{e\}$, then $(H \times K)/K \cong H$.

We turn now to the main result. I've pretty much followed the treatment given by R. Hirshon, in his paper *Decomposition of groups,* in the AMERICAN MATHEMATICAL MONTHLY, vol. 76 (1969), pp. 1037-1039.

Theorem 7. [Cancellation of Finite Groups] *Assume that we have an isomorphism $H \times L \cong K \times G$, where $L \cong G$ and are finite groups. Then $H \cong K$.*

Proof. We shall regard the above direct product as internal. Assume that $\phi : H \times L \to K \times G$ is an isomorphism. Thus, if $K' = \phi(H)$, $G' = \phi(L)$, then we have $K' \times G' = K \times G$; the task, then, is to show that $K \cong K'$. We now set $X = K \times G = K' \times G'$; since we have regarded the direct products as internal, then K, K', G, G' are all normal subgroups of X, and $G \cong G'$.

We divide the proof into two steps.

Step 1. *If $K' \cap G = \{e\}$, or if $K \cap G' = \{e\}$, we shall show that $K' \cong K$.* In the first case, we have $K'G = K' \times G \leq X = K' \times G'$. However, $|G| = |G'|$ and so the index of K' in both $K' \times G$ and $K' \times G'$ is the same. Therefore, $K' \times G = K' \times G' = K \times G$, and so

$$K' \;\cong\; (K' \times G)/G \;=\; (K \times G)/G \;\cong\; K.$$

The argument is similar in case $K \cap G' = \{e\}$.

Step 2. *Induction on $|G|$.)* Set $M = K \cap G'$, $N = K' \cap G$, and note that $M, N \triangleleft X$, and that $M \cap N = \{e\}$. We have

$$X/(M \times N) \;=\; (K \times G)/(M \times N) \;\cong\; (K/M) \times (G/N),$$

and

$$\begin{aligned} X/(M \times N) \;=\; X/(N \times M) \;&=\; (K' \times G')/(N \times M) \\ &\cong\; (K'/N) \times (G'/M). \end{aligned}$$

Therefore $(K/M) \times (G/N) \cong (K'/N) \times (G'/M)$. But $G \cong G'$ and so

$$G \times (K/M) \times (G/N) \;\cong\; G' \times (K'/N) \times (G'/M). \qquad (*)$$

We now work on the right hand side of (*):

$$\begin{aligned} G' \times (K'/N) \times (G'/M) \;&\cong\; ((G' \times K')/N) \times (G'/M) \\ &=\; ((G \times K)/N) \times (G'/M) \\ &\cong\; (G/N) \times K \times (G'/M) \\ &\cong\; K \times (G/N) \times (G'/M), \end{aligned}$$

In other words,

$$G' \times (K'/N) \times (G'/M) \;\cong\; K \times (G/N) \times (G'/M). \qquad (**a)$$

In an entirely similar way,

$$G \times (K/M) \times (G/N) \;\cong\; K' \times (G'/M) \times (G/N). \qquad (**b)$$

Now apply (*) to the left hand sides of (**a) and (**b) and infer that

$$K \times (G/N) \times G'/M) \;\cong\; K' \times (G/N) \times (G'/M).$$

By induction we may successively cancel (G'/M) and then (G/N), resulting in the desired isomorphism: $K \cong K'$.

Corollary. [Uniqueness of Invariant Factors] *Let A be a finite abelian group with invariant factors $n_1, n_2, \ldots, n_s$, and $m_1, m_2, \ldots, m_t$. Then $s = t$ and $m_i = n_i,\ i = 1, 2, \ldots, s$.*

Proof. By assumption, we have

$$Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s} \cong A \cong Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_t},$$

where $n_{i+1}|n_i,\ i = 1, 2, \ldots, s-1$, and $m_{j+1}|m_j,\ j = 1, 2, \ldots, t-1$. Note that if $n_1 \neq m_1$, say $m_1 < n_1$, then since $A \cong Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_t}$, we conclude that $a^{m_1} = e$ for all $a \in A$. However, as A contains a subgroup isomorphic with Z_{n_1}, then A has an element of order n_1, a contradiction. Therefore, $n_1 = m_1$. Now use induction on $|A|$ and apply *Theorem* 7, to cancel off the Z_{n_1} factors and infer that the remaining invariant factors all agree.

Example 1. The possible isomorphism types of abelian groups of order 16 are:

$$Z_{16},\ Z_8 \times Z_2,\ Z_4 \times Z_4,\ Z_4 \times Z_2 \times Z_2,\ Z_2 \times Z_2 \times Z_2 \times Z_2.$$

Example 2. The possible isomorphism types of abelian groups of order 100 are

$$Z_{100},\ Z_{50} \times Z_2,\ Z_{20} \times Z_4,\ Z_{10} \times Z_{10}.$$