Group Theory - Week 6 - Decomposing Finite Abelian Groups

Antonio León Villares

October 2022

Contents

Based on the notes by Susan J. Sierra, Section 5.1

1 Abelian Groups from Direct Products

1.1 Internal Direct Products

1.1.1 Definition: Internal Direct Products

*Let G be a **group**, with $H, K \triangleleft G$. Then, G is the **internal direct product** of H and K if:*

1.
$$G = HK = \{hk \mid h \in H, k \in K\}$$

2.
$$H \cap K = \{e\}$$

3.
$$\forall h \in H, k \in K, \qquad hk = kh$$

---

*A more general statement can be found here, where for a **internal direct product**, given $H_i, i \in [1, n]$ **subgroups** of G we require that:*

1. $G = H_1 H_2 \dots H_n$
2. $H_i \triangleleft G$
3. $\hat{H}_i = H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n \implies H_i \cap \hat{H}_i = \{e\}$

and they show that the commutativity condition $h_i h_j = h_j h_i$ follows from the above properties.

1.1.2 Theorem: Internal Direct Products are Isomorphic to External Direct Products

*Let G be a group with $H, K \triangleleft G$, such that G is an **internal direct product** of H and K. Then:*

$$G \cong H \times K$$

*More generally, if G is a **internal direct product** of n groups H_i, then:*

$$G \cong H_1 \times H_2 \times \dots \times H_n$$

We prove the claim for $n = 2$, with the more general claim following by an inductive argument.

Define a homomorphism:

$$\phi : H \times K \to G$$

via:

$$\phi(h, k) = hk$$

We claim that ϕ is an **isomorphism**.

① **Injectivity**

Let $(h, k) \in ker(\phi)$. That is:

$$\phi(h, k) = hk = e$$

This is true **if and only if**:

$$h = k^{-1}$$

But H, K are subgroups, which are closed under inverses, and since $H \cap K = \{e\}$, we know that $h \notin K$ unless $h = e$. Hence, we must have that:

$$(h, k) = (e, e)$$

Thus, $ker(\phi) = \{e\}$, and ϕ is injective.

② **Surjectivity**

Let $g \in G$. Since G is an internal direct product, $\exists h \in H, k \in K$ such that:

$$g = hk$$

Hence:

$$\phi(h, k) = g$$

and ϕ is surjective.

③ **Homomorphism**

Let $(h_1, k_1), (h_2, k_2) \in H \times K$. Then:

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi(h_1h_2, k_1k_2) \\ &= (h_1h_2)(k_1k_2) \\ &= (h_1k_1)(h_2k_2), \quad \textit{(since } hk = kh \textit{ by assumption of IDP)} \\ &= \phi(h_1, k_1)\phi(h_2, k_2)\end{aligned}$$

so ϕ is a homomorphism.

Thus, we have shown that ϕ defines an isomorphism, and so:

$$H \times K \cong G$$

as required.

1.2 Constructing Abelian Groups from Sylow Subgroups

1.2.1 Lemma: Order of Group Products

Let H, K be ***finite*** *subgroups of G. Then:*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. We can partition HK by using cosets:

$$HK = \cup_{h \in H} hK$$

This is because clearly $K \leq H$, and any element $hk \in HK$ must belong to a given coset hK.

Since cosets are either identical ($h_1 K = h_1' K$) or disjoint ($h_1 K \cap h_2 K = \emptyset$), we see that $|HK|$ will be defined by the number of **distinct** cosets of K.

Let's assume 2 cosets are equal. That is, we have for $h, h' \in H, h \neq h'$:

$$hK = h'K \implies h'^{-1}h \in K$$

By subgroup closure $h'^{-1}h \in H$, so we must have:

$$h'^{-1}h \in H \cap K$$

Moreover, $\forall k \in K$, defining $h' = hk$ ensures that $h'K = hK$. In other words, for each element $h \in H$, if $h \in H \cap K$, we are overcounting it by a factor of $|H \cap K|$ (since there are $|H \cap K|$ many elements ensuring that if $h' \in H \cap K$, then $\exists k \in K$ such that $h' = hk$, so we will have equal cosets). Hence, the total number of distinct cosets will be:

$$\frac{|H|}{|H \cap K|}$$

Since each coset is such that $|hK| = |K|$, it follows that:

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

as required.

□

1.2.2 Lemma: Order of an Element as the Greatest Common Divisor

Let G be a group and $g \in G$. If:

$$g^{\alpha} = g^{\beta} = e$$

then:

$$g^{gcd(\alpha,\beta)} = e$$

Proof. Recall Bezout's Lemma, which states that if d is the greatest common divisor of $x, y \in \mathbb{Z}$, then $a, b \in \mathbb{Z}$ such that:

$$ax + by = d$$

Hence:

$$\begin{aligned} g^{gcd(\alpha,\beta)} &= g^{a\alpha + b\beta} \\ &= g^{a\alpha} g^{b\beta} \\ &= (g^{\alpha})^a \left(g^{\beta}\right)^b \\ &= e^a e^b \\ &= e \end{aligned}$$

as required.

□

We are now ready to prove the main theorem of this section: we can deconstruct finite abelian groups by using its Sylow subgroups.

1.2.3 Theorem: Abelian Group is Isomorphic to Direct Product of Sylow Subgroups

Suppose that A is a ***finite abelian group*** *of order n, where:*

$$n = \prod_{i=1}^{k} p_i^{s_i}$$

where p_i are distinct primes, and $s_i \in \mathbb{N}$.
Let A_{p_i} be the ***unique*** *Sylow p_i-subgroup of A.*
Then:

$$A \cong A_{p_1} \times A_{p_2} \times \ldots \times A_{p_k}$$

(Theorem 5.1.3)

Notice, here we are saying that A_{p_i} are ***unique****. This is due to the fact that G is abelian, so any subgroup H is* ***normal****:*

$$gHg^{-1} = gg^{-1}H = H$$

so by Sylow II, it follows that n_{p_i} = number of conjugate Sylow p_i subgroups = 1.

Proof. If we can show that G is an internal direct product of its Sylow p-subgroups, then by the Theorem above, G will be isomorphic to the direct product of its Sylow p-subgroups.

Notice, the Sylow p_i-subgroups are automatically normal by definition (since they are unique), so this satisfies property 2 of IDPS.

We now claim that if $A = A_{p_1} \dots A_{p_{i-1}} A_{p_{i+1}} \dots A_{p_k}$, then:

$$A_{p_i} \cap A = \{e\}$$

We do so by induction. In the case $k = 2$, we only have 2 Sylow p-subgroups, so we consider $A_{p_1} \cap A_{p_2}$. If $g \in A_{p_1} \cap A_{p_2}$, then:

$$g \in A_{p_1} \implies g^{|A_{p_1}|} = g^{p_1^{s_1}} = e$$

$$g \in A_{p_2} \implies g^{|A_{p_2}|} = g^{p_2^{s_2}} = e$$

But then, by the Lemma above, it follows that:

$$g^{gcd(p_1^{s_1}, p_2^{s_2})} = e$$

But since p_1, p_2 are prime, they (and their powers) will be coprime, so $g^1 = e$ and $g = e$. So we verify the case $k = 2$.

Now, assume true for $k = m$, and consider the case $k = m+1$, where $g \in A_i \cap A$. By inductive hypothesis, we know that $\bigcap_{j=1, j \neq i}^{m+1} A_{p_j} = \{e\}$. In other words, by the Lemma on the order of product groups:

$$|A| = \prod_{j=1, j \neq i}^{m+1} |A_{p_j}| = \prod_{j=1, j \neq i}^{m+1} p_j^{s_j}$$

Then:

$$g \in A_{p_i} \implies g^{p_i^{s_i}} = e$$

$$g \in A \implies g^{\prod_{j=1, j \neq i}^{m+1} p_j^{s_j}} = e$$

But then:

$$g^{gcd\left(g^{p_i^{s_i}}, \prod_{j=1, j \neq i}^{m+1} p_j^{s_j}\right)} = e$$

and since all the values are coprime, we again get $g^1 = e$. Hence:

$$A_{p_i} \cap A = \{e\}$$

and thus, we have proven property 3 of IDPs.

We now need to show that:

$$G = A_{p_1} A_{p_2} \dots A_{p_k}$$

Notice, since:

$$A_{p_1} A_{p_2} \dots A_{p_k} \leq G$$

it suffices to show that:

$$|G| = |A_{p_1} A_{p_2} \dots A_{p_k}|$$

But notice, since we have property 3 proven, we know that:

$$\bigcap_{i=1}^{k} A_{p_i} = \{e\}$$

so:

$$|A_{p_1} A_{p_2} \dots A_{p_k}| = \frac{\prod_{i=1}^{k} |A_{p_i}|}{\left|\bigcap_{i=1}^{k} A_{p_i}\right|} = \prod_{i=1}^{k} p_i^{s_i} = |G|$$

Hence, we also have property 1.

Hence, G is a internal direct product of its Sylow subgroups, and so:

$$A \cong A_{p_1} \times A_{p_2} \times \dots \times A_{p_k}$$

as required.

□

1.3 Theorem: Abelian Group of Prime Power Order is Isomorphic to Direct Product of Cyclic Subgroups

Let A be an ***abelian group*** *with prime-power order:*

$$|A| = p^n$$

Then, A is ***isomorphic*** *to the* ***direct product*** *of* ***cyclic subgroups*** *with orders:*

$$p^{e_1}, \dots, p^{e_s}$$

where:

$$e_1 \geq e_2 \geq \dots \geq e_s \geq 1$$

and:

$$\sum_{i=1}^{s} e_i = n$$

This product is ***unique*** *up to reordering of the factors.*
(Theorem 5.1.4)

1.4 Corollary: Fundamental Theorem of Finite Abelian Groups (I)

Let A be a ***finite abelian group****. Then, A is a* ***direct product*** *of* ***cyclic groups*** *of* ***prime power order****. This product is* ***unique*** *up to reordering of the factors.*
(Corollary 5.1.5)

Proof. We can decompose A into a direct product of its Sylow p-subgroups, each of which with order $p_i^{s_i}$. By the above Theorem, we can then further decompose each of the Sylow p-subgrouops into a direct product of cyclic subgroups with orders $p_i^{e_j}$. Hence, we can decompose A into a direct product of cyclic groups of prime power order, as required. □

1.5 Theorem: Chinese Remainder Theorem

*Let m, n be non-zero **coprime** integers. Then:*

$$C_{mn} \cong C_m \times C_n$$

(Theorem 5.1.6)

This theorem was stated without proof in week 1

Proof. Let:

$$C_m = \langle a \rangle \qquad C_n = \langle b \rangle$$

and define the following homomorphism:

$$\phi : \mathbb{Z} \to C_m \times C_n$$

via:

$$\phi(r) = (a^r, b^r)$$

This is a homomorphism, since:

$$\begin{aligned} \phi(r_1 + r_2) &= (a^{r_1+r_2}, b^{r_1+r_2}) \\ &= (a_1^r a_2^r, b_1^r, b_2^r) \\ &= (a_1^r, b_1^r)(a_2^r, b_2^r) \\ &= \phi(r_1)\phi(r_2) \end{aligned}$$

Now, consider the kernel of ϕ. In particular, $r \in ker(\phi)$ if:

$$\phi(r) = (e, e) \iff a^r = b^r = e$$

In other words, r must be the smallest natural number which is a multiple of both m and n (which are the respective orders of a and b). In other words:

$$r = lcm(m, n)$$

But m, n are coprime, so:

$$r = mn$$

Hence:

$$ker(\phi) = mn\mathbb{Z}$$

Now, we apply the **First Isomorphism Theorem**:

$$\mathbb{Z}/mn\mathbb{Z} \cong im(\phi)$$

But notice:

$$\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}_{mn} \cong C_{mn}$$

Moreover:

$$|im(\phi)| = |C_{mn}| = mn = |C_m \times C_n|$$

so it follows that ϕ must be an isomorphism, and so:

$$C_{mn} \cong C_m \times C_n$$

as required.

□

1.6 Corollary: Fundamental Theorem of Finite Abelian Groups (II)

Any ***finite abelian group*** *A of order n can be written as a* ***direct product*** *of* ***cyclic groups****:*

$$A = C_{n_1} \times C_{n_2} \times \ldots \times C_{n_s}$$

where:

- $\forall i \in [1, s-1], \qquad n_i \mid n_{i+1}$
- $\prod_{i=1}^{s} n_i = n$

This product is ***unique*** *up to reordering of the factors.*
(Corollary 5.1.8)

1.7 Worked Examples

1.7.1 Decomposing the Cyclic Group of Order 100

Consider the cyclic group C_{100}. We have $100 = 2^2 \times 5^2$, so Sylow I tells us we should expect a Sylow 2-subgroup of order 4, and a Sylow 5-subgroup of order 25.

By the Fundamental Theorem of Finite Abelian Groups (I), we can write C_{100} as a direct product of prime power subgroups. This gives us the 4 following possibilities:

- $C_4 \times C_{25}$
- $C_2 \times C_2 \times C_{25}$
- $C_2 \times C_2 \times C_5 \times C_5$
- $C_4 \times C_5 \times C_5$

By the Fundamental Theorem of Finite Abelian Groups (II), we can also write C_{100} as a direct product of mutually "divisible" cyclic groups. Indeed, using the Chinese Remainder Theorem, we see that:

- $C_4 \times C_{25} \cong C_{100}$
- $C_2 \times C_2 \times C_{25} \cong C_2 \times C_{50}$
- $C_2 \times C_2 \times C_5 \times C_5 \cong C_{10} \times C_{10}$
- $C_4 \times C_5 \times C_5 \cong C_5 \times C_{20}$

1.7.2 Finding Abelian Groups of Order 540

The following is an exercise from the August 2019 exam

- **Up to isomorphism, how many abelian groups are there of order 540? Give 2 different lists of these groups, using the 2 versions of the Fundamental Theorem of Finite Abelian Groups, and indicate which groups on the 2 lists are isomorphic?**
- **Let A be an abelian group of order 540 which has no elements of order 20 or 18. How many elements of order 30 does A have? Justify your answer with a proof.**

Assume A is an abelian group of order 540. We can write:

$$540 = 2 \times 5 \times 6 \times 9 = 2^2 \times 3^3 \times 5$$

so A has 3 Sylow subgroups: a Sylow 2-subgroup of order 4, a Sylow 3-subgroup of order 27 and a Sylow 5-subgroup of order 5.

By the Fundamental Theorem of Finite Abelian Groups (I), we can write A as a direct product of prime power orders. Thus, we get the following options:

- $C_4 \times C_{27} \times C_5$
- $C_2 \times C_2 \times C_{27} \times C_5$
- $C_4 \times C_3 \times C_3 \times C_3 \times C_5$
- $C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5$
- $C_4 \times C_3 \times C_9 \times C_5$
- $C_2 \times C_2 \times C_3 \times C_9 \times C_5$

(these are unique up to reordering, so these are the only possible options)

By using the Chinese Remainder Theorem, we get the cyclic groups from the Fundamental Theorem of Finite Abelian Groups (II) (recall, the order of the cyclic subgroups must divide each other):

- $C_4 \times C_{27} \times C_5 \cong C_{540}$
- $C_2 \times C_2 \times C_{27} \times C_5 \cong C_2 \times C_{270}$
- $C_4 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_3 \times C_3 \times C_{60}$
- $C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_3 \times C_6 \times C_{30}$

- $C_4 \times C_3 \times C_9 \times C_5 \cong C_3 \times C_{180}$
- $C_2 \times C_2 \times C_3 \times C_9 \times C_5 \cong C_6 \times C_{90}$

Now assume that $|A| = 540$ and that A has no element of order 20 or 18. By CRT, elements of order 20 arise as a result of $C_4 \times C_5$, whilst groups or order 18 arise as a result of $C_2 \times C_9$. This means that the following groups can't be A:

- $C_4 \times C_{27} \times C_5$
- $C_4 \times C_3 \times C_3 \times C_3 \times C_5$
- $C_4 \times C_3 \times C_9 \times C_5$
- $C_2 \times C_2 \times C_3 \times C_9 \times C_5$

This leaves only 2 possibilities:

- $C_2 \times C_2 \times C_{27} \times C_5$
- $C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5$

But now, we require a group with elements of order 30. We see that the only group satisfying this is:

$$C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_3 \times C_6 \times C_{30}$$

since:

$$C_2 \times C_2 \times C_{27} \times C_5 \cong C_2 \times C_{270}$$

The elements of order 30 arise from the direct product:

$$(C_2 \times C_2) \times (C_3 \times C_3 \times C_3) \times C_5$$

From C_5, there are 4 possible elements of order 5 (discounting the identity). From $C_3 \times C_3 \times C_3$, we get 26 elements of order 3 (discounting the identity). Finally, from $C_2 \times C_2$ we have 3 elements of order 2 (discounting the identity). Thus, we have:

$$4 \times 3 \times 26 = 312$$

elements of order 30.

2 The Exponent

2.1 Definition: The Exponent of a Group

> *Let G be a group. We denote with $e(G)$ the **exponent** of G. $e(G)$ is the **least common multiple** of the **orders** of the elements of G*

For example, in S_3 the elements have order 1, 2 or 3, so $e(S_3) = 6$.

2.2 Lemma: Exponent Bounded by Group Order

For any finite group G:

$$e(G) \leq |G|$$

Proof. Let G be a group. By Lagrange's Theorem, the order $o(g)$ of any element $g \in G$ divides $|G|$. If all the orders of the group are coprime (ignoring group elements with repeated orders, since repeated orders won't contribute to changing the lcm), then:

$$e(G) = |G|$$

(this is the case of S_3 shown above)

Otherwise, there are at least 2 elements g_1, g_2 such that $o(g_1) \neq o(g_2)$ are not coprime. WLG, we can assume $o(g_2) > o(g_1)$, which means that:

$$e(G) < |G|$$

This is because the lcm of the remaining elements will be the product of all the (distinct) orders, call it ℓ; however, $lcm(o(g_1), o(g_2)) = o(g_2) < o(g_1)o(g_2)$. Thus:

$$e(G) = \ell \times o(g_2) < \ell \times o(g_1)o(g_2) \leq |G|$$

(for example, in D_4 group elements have order 1,2,4, so $e(D_4) = 4 \neq 8$)

□

2.3 Lemma: Abelian Groups Contain Elements with Order which Divides Exponent

Let A be a ***finite abelian group****.*
If k divides $e(A)$, then:

$$\exists g \in A \ : \ o(g) = k$$

Proof. Say that $km = e(A)$, and $a \in A$ has order $e(A)$. Then:

$$a^{e(A)} = e \implies (a^m)^k = e$$

so $a^m \in A$ is an element of order k

□

The above Lemma is really useful for "filtering" out abelian groups if we have some group order restriction. For example, in the problem above with abelian groups of order 540, we found the following possibilities:

- $C_4 \times C_{27} \times C_5 \cong C_{540}$
- $C_2 \times C_2 \times C_{27} \times C_5 \cong C_2 \times C_{270}$
- $C_4 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_3 \times C_3 \times C_{60}$
- $C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_3 \times C_6 \times C_{30}$
- $C_4 \times C_3 \times C_9 \times C_5 \cong C_3 \times C_{180}$
- $C_2 \times C_2 \times C_3 \times C_9 \times C_5 \cong C_6 \times C_{90}$

We imposed the restriction of having no group of order 20 or 18. Consider, for example, $C_6 \times C_{90}$. It is immediate that the exponent of this group is 90 (we imposed that if $A = C_{n_1} \times C_{n_2} \times \ldots \times C_{n_s}$, then $n_i \mid n_{i+1}$, so n_s must be divisible by all previous group orders, and each such group contains an element of order n_i, so n_s must be the lcm).
This then tells us $C_6 \times C_{90}$ will have elements of orders which divide 90, namely:

$$1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90$$

so $C_6 \times C_{90}$ will contain an element of order 18.

2.4 Lemma: Abelian Groups Contain Elements with Exponent Order

*Let A be a **finite abelian group**.*
Then A contains an element of order $e(A)$.
(Lemma 5.1.11)

Proof. First, assume that A is a group of order p^m, where p is prime. Let $a \in A$ be such that:

$$o(a) = p^s, \quad s \leq m$$

such that a is the element of highest order. Then, by Lagrange's Theorem, any other element of A must have order:

$$p^t, \quad s \leq t$$

Hence, it follows that $e(A) = p^s$.

Now, consider a general abelian group A. We can decompose A into a direct product of its Sylow p-subgroups:

$$|A| = n = \prod_{i=1}^{k} p_i^{s_i} \implies A \cong A_{p_1} \times \ldots \times A_{p_k}$$

Now, let $a \in A_{p_1} \times \ldots \times A_{p_k}$. Each subgroup has coprime order, so by the Chinese Remainder Theorem we know that:

$$a = (a_1, \ldots, a_k) \implies o(a) = \prod_{i=1}^{k} o(a_i)$$

Now, pick the components of a, such that a_i is the element of greatest order in A_{p_i}, say $o(a_i) = p_i^{t_i}$. Then:

$$e(A_{p_i}) = o(a_i) = p_i^{t_i}$$

In particular, any element in A must have order less than or equal to:

$$\prod_{i=1}^{k} p_i^{t_i}$$

(since the orders are all coprime), and so:

$$e(A) = \prod_{i=1}^{k} p_i^{t_i}$$

and thus, $a \in A$ is an element of order $e(A)$ as required.

□

2.5 Corollary: Abelian Group with Exponent Order is Cyclic

If A is a ***finite abelian group*** *with:*

$$e(A) = |A|$$

then A is cyclic.
(Corollary 5.1.12)

Proof. Since $e(A) = |A|$, then $\exists a \in A$ such that $o(a) = |A|$ by the Theorem above. But then, this is true **if and only if** A is cyclic (the subgroup generated by a has order $|A|$, so $\langle a \rangle = A$, and A is cyclic). □

2.6 Theorem: Subgroup of Multiplicative Field is Cyclic

Let A be a ***finite subgroup*** *of the* ***multiplicative group****:*

$$K^* = K \setminus \{0\}$$

of a ***field*** *K. Then A is a* ***cylic group****.*
In particular, K^* will be ***cyclic****.*
(Theorem 5.1.13 & Corollary 5.1.14)

Recall, a field is a ***non-zero, commutative ring****, where each non-zero element has a* ***multiplicative inverse****. Moreover, a* ***ring*** *is a set:*

$$(R, +, \cdot)$$

such that:

1. $(R, +)$ *is an* ***abelian group****, with identity* 0_R
2. $(R, \cdot)$ *is a* ***monoid****:*
   - *multiplication is* ***associative***
   - *there is an identity element* 1_R*:*

$$\forall a \in R, \quad a \cdot 1_R = 1_R \cdot a = a$$

3. ***distributive laws*** *hold in* R*:*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Proof. Since K is a field, in particular it is a commutative group under multiplication, so any subgroup will also be commutative. Thus, A will be abelian.

Now, define:

$$e = e(A)$$

Since e is the lowest common multiple of the order of all group elements, we must have:

$$\forall a \in A, \qquad a^e = 1$$

(1 is the multiplicative identity)

In particular, working with the ring of polynomials over K, $K[X]$, it follows that all the elements of A are roots of:

$$X^e - 1 \in K[X]$$

Since $X^e - 1$ has at most e roots, it follows that:

$$|A| \leq e$$

But recall, a property of the exponent is that $e \leq |A|$. Hence, we must have that $e = |A|$. By the Corollary above, A must be a cyclic subgroup, as required.

□