PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 10

INSTRUCTOR: ARUNDHATHI KRISHNAN

11. Fundamental Theorem of Finite Abelian Groups

The goal of this lecture is to establish the fundamental theorem for finite Abelian groups. This is a result that describes the structure of all Abelian groups of finite order, up to isomorphism. We first state the theorem.

Theorem 11.0.1 (Fundamental Theorem)**.** *Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the direct product and the orders of the cyclic groups are uniquely determined by the group.*

The above theorem implies that for any finite Abelian group G, we have the following:

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}},$$

where the p_i-s are not necessarily distinct and the prime-powers $p_1^{n_1}, \ldots, p_k^{n_k}$ are uniquely determined by G. Expressing G as such a direct product is known as *determining the isomorphism classes of* G.

We delay the proof of the fundamental theorem for the time being, and consider some applications first.

11.1. The isomorphism classes of Abelian groups.

We will use the fundamental theorem to construct Abelian groups of any order. First, suppose the group has order p^k where p is a prime and k is a positive integer. Suppose k can be written as a sum of positive integers:

$$k = n_1 + \cdots n_t.$$

The set of positive integers $\{n_1, \ldots, n_t\}$ is called a partition of k, and each partition gives rise to the following Abelian group of order p^k:

$$\mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}},$$

Further, the fundamental theorem gives that each partition yields a distinct isomorphism class of finite Abelian groups. Let us consider some concrete constructions for $k = 1$, 2, 3 and 4.

Order of G	k	Partitions of k	Possible direct products for G
p	1	1	$\mathbb{Z}_p$
p^2	2	2	$\mathbb{Z}_{p^2}$
		$1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	3	$\mathbb{Z}_{p^3}$
		$2+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
		$1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^4	4	4	$\mathbb{Z}_{p^4}$
		$3+1$	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
		$2+2$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
		$2+1+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
		$1+1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

The fundamental theorem makes it remarkably easy to classify all Abelian groups of a given order. The non-Abelian case is much harder, even for small orders. Now that we have described how to use partitions to construct Abelian groups of prime-power order, we move to the general case of *any* finite order, say n. We first write the prime-power decomposition of n, say

$$n = p_1^{n_1} \cdots p_k^{n_k}.$$

Then we form all the Abelian groups of order $p^{n_1}, \ldots, p_k^{n_k}$ as outlined above using partitions. Finally, we put them together to form all possible external direct products of these groups.

Let's try an example. Say $|G| = 7938 = 2 \times 3^4 \times 7^2$. The prime-power 2 gives us $\mathbb{Z}_2$, 3^4 gives us one of $\mathbb{Z}_{81}$, $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$, $\mathbb{Z}_9 \oplus \mathbb{Z}_9$, $\mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, and the prime-power 7^2 gives either $\mathbb{Z}_{49}$ or $\mathbb{Z}_7 \oplus \mathbb{Z}_7$. So G must be (isomorphic to) one of the following:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{49}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{49}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$$

In practice, given a group of order 7938, how do we know which of the following ten options it is equal to? One could, for instance, compare the number of elements of given orders to narrow it down. For instance, if G has an element of order 49, it must be the first, third, fifth, seventh or ninth option above. If we know that G has an element of order 81, then it must be isomorphic to the first or second option.

How do we express a finite Abelian group G as an *internal* direct product? We will see the following construction in the proof of the fundamental theorem. Suppose we have a group of order 2^n. Pick an element a_1 of maximum order, say 2^r. Then $\langle a_1 \rangle$ is one of the factors in the internal direct product. If $G \neq \langle a_1 \rangle$, choose an element a_2 of maximum order 2^s such that $s \leq n - r$ and none of $a_2, a_2^2, a_2^4, \ldots, a_2^{2^{s-1}}$ is in $\langle a_1 \rangle$. Then $\langle a_2 \rangle$ is another direct factor. If $G \neq \langle a_1 \rangle \times \langle a_2 \rangle = \{a_1^i a_2^j \mid 0 \leq i < 2^r, 0 \leq j < 2^s\}$, then choose a_3 of maximum order 2^t such

that $t \leq n-r-s$ and none of $a_3, a_3^2, \ldots, a_3^{2^{t-1}}$ is in $\langle a_1\rangle \times \langle a_2\rangle$. Then $\langle a_3\rangle$ is another direct factor. We continue in this manner until our direct product has the same order as G.

In general, for a prime p and a group of order p^n, we do the following:

(i) Pick an element a_1 of maximum order, say p^r. Then $\langle a_1\rangle$ is one of the factors in the internal direct product.

(ii) If $G \neq \langle a_1\rangle$, choose an element a_2 of maximum order p^s such that $s \leq n-r$ and none of $a_2, a_2^p, a_2^{p^2}, \ldots, a_2^{p^{s-1}}$ is in $\langle a_1\rangle$. Then $\langle a_2\rangle$ is another direct factor.

(iii) Continue in this manner until the direct product has the same order as G.

If the order of G is $n = p_1^{n_1} \cdots p_k^{n_k}$, then we build the pieces for each prime and put them together as an internal direct product.

Example 11.1.1. Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ under multiplication modulo 65. G has order $16 = 2^4$, hence we know it is isomorphic to one of

$$\mathbb{Z}_{16}$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

To decide which of the five options G must be isomorphic to, we list the orders of its elements:

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

As the only possible orders are 1, 2 and 4, we can rule out the first two and the last options. It is not hard to compute that $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has only 8 elements of order 4, whereas G has 12. So G must be isomorphic by elimination to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

We also show how to express G as an internal direct product. Choose 8, say, which has the maximum order $4 = 2^2$, so $\langle 8\rangle$ is one factor. Next, choose some element a which has maximal order and $a, a^2 \notin \langle 8\rangle = \{8, 64, 57, 1\}$, say $a = 12$. Then $G = \langle 8\rangle \times \langle 12\rangle$.

It is of course not always practical to compute the order of every element of a given group. Sometimes, it may be enough to find the order of just a few elements.

Example 11.1.2. Let

$$G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\},$$

under multiplication modulo 135.

As $|\,G\,| = 24 = 2^3 \times 3$, G must be isomorphic to one of the following:

$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24}$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

The element 8 has order 12, so the last option is ruled out. The elements 109 and 134 both have order 2, so the group cannot be cyclic (as it has two subgroups of order 2). Hence G must be isomorphic to $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$. So G can be expressed as $G = \langle 8\rangle \times \langle 134\rangle$.

To express G as an internal direct product using our algorithm, we see that as $G \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$, the maximum order an element can have of power 2 is 4, say for instance, 28. Hence $\langle 28\rangle$ is one factor, and we can choose an element of order 2, say 134 which is not in $\{1, 28, 109, 82\}$. Then $\langle 28\rangle \times \langle 134\rangle$ takes care of the powers of 2. The element 46 is of order 3, so we get $G = \langle 28\rangle \times \langle 134\rangle \times \langle 46\rangle$. This is isomorphic to the direct product we have already obtained.

The fundamental theorem gives us the following corollary, which is a converse of Lagrange's theorem for finite Abelian groups.

Corollary 11.1.3. *If m divides the order of a finite Abelian group G, then G has a subgroup of order m.*

It is illustrative to verify this with an example, and convince yourself that you can indeed write a proof in the general case!

Example 11.1.4. Suppose G is an Abelian group of order $72 = 2^3 \times 3^2$. We will find a subgroup of G of order 12. By the fundamental theorem G must be isomorphic to one of the following six groups:

$$\begin{array}{ll} \mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72} & \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24} \oplus \mathbb{Z}_3 \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36} \oplus \mathbb{Z}_2 & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \end{array}$$

It is clear that one can find a subgroup of order 12 in the first four cases, since there is a cyclic group whose order is a multiple of 12 sitting in the direct product $(\mathbb{Z}_{72}, \mathbb{Z}_{24}, \mathbb{Z}_{36}, \mathbb{Z}_{12})$. Let us try to find subgroups in the last two cases which have order 12. Clearly, $\langle 6 \rangle \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a subgroup of order 12 in $\mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_6 \oplus \{0\} \oplus \mathbb{Z}_2$ has order 12 in $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

11.2. **Proof of the fundamental theorem.** We will prove the fundamental theorem via a series of lemmas.

Lemma 11.2.1. *Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|\, H \,| = p^n$.*

Proof. Any set of the form $\{x \in G \mid x^l = e\}$ for some integer l is a subgroup, as $e^l = e$ and $x^l = y^l = e$ implies that $(xy^{-1})^l = x^l y^{-l} = e$ as G is Abelian. Hence, H and K are subgroups.

We will now prove that $G = HK$ and $H \cap K = \{e\}$. The latter follows easily as $x \in H \cap K$ implies that $x^{p^n} = e = x^m$, so that $|\, x \,|$ divides m and p^n. But as p is prime and does not divide m, it must hold that $|\, x \,| = 1$ and $x = e$.

Let $x \in G$. As $\gcd(m, p^n) = 1$, there exist $s, t \in \mathbb{Z}$ such that $sm + tp^n = 1$, so that $x = x^{sm+tp^n} = x^{sm} x^{tp^n}$. Now, $x^{sm} \in H$ as $(x^{sm})^{p^n} = x^{s|\,G\,|} = e$; similarly, $x^{tp^n} \in K$, so $x \in HK$.

Finally, $p^n m = |\, HK \,| = |\, H \,|\,|\, K \,|$. If p divides $|\, K \,|$, then K has an element of order p by Cauchy's Theorem (9.3.4). Hence p divides m, a contradiction. So it must hold that $|\, H \,| = p^n$.

□

Repeated applications of Lemma 11.2.1 give the following. Let G be an Abelian group with $|\, G \,| = p_1^{n_1} \cdots p_k^{n_k}$, where the p_i-s are distinct primes. Then taking $G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$,

$$G = G(p_1) \times \cdots \times G(p_k),$$

and $|\, G(p_i) \,| = p_i^{n_i}$.

We will now further decompose each $G(p_i)$.

Lemma 11.2.2. *Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a \rangle \times K$ for some subgroup K.*

Proof. Let $|\,G\,| = p^n$. We will prove the result by induction on n. If $n = 1$, then $|\,G\,| = p$ and $|\,a\,| = p$, so that $G = \langle a\rangle \times \langle e\rangle$.

Next, suppose that the statement is true for all Abelian groups of order p^k, where $k < n$. Choose an element a of maximum order p^m. Then $x^{p^m} = e$ for all $x \in G$ (as the order of any element must be a power of p and p^m is the highest among such orders). If $G = \langle a\rangle$, we are done.

Otherwise, choose b of smallest order such that $b \notin \langle a\rangle$. We claim that $\langle a\rangle \cap \langle b\rangle = \{e\}$. Since $|\,b^p\,| = \frac{|\,b\,|}{p} < |\,b\,|$, we know that $b^p \in \langle a\rangle$. Suppose $b^p = a^i$, then $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^m-1}$, so that $\left|\,a^i\,\right| \leq p^{m-1}$. Hence a^i is not a generator of $\langle a\rangle$, so that $\gcd(p^m, i) \neq 1$. This implies that p divides i, so that $i = pj$ for some integer j. Hence $b^p = a^i = a^{pj}$. Let $c = a^{-j}b$. Then $c \notin \langle a\rangle$, and $c^p = a^{-jp}b^p = e$. We have thus found an element c of order p with $c \notin \langle a\rangle$, so by the way we have chosen b, it must hold that $|\,b\,| = p$.

Now, suppose $x \in \langle a\rangle \cap \langle b\rangle$. If $x \neq e$, then x generates $\langle b\rangle$ so that $b \in \langle a\rangle$, a contradiction. Hence the intersection is $\{e\}$.

Now, let $\overline{G} := {}^{G}\!/_{\langle b\rangle}$ and write any coset $x\langle b\rangle$ as $\overline{x}$. If $|\,\overline{a}\,| < |\,a\,| = p^m$, then $\overline{a}^{p^{m-1}} = \overline{e}$, hence $a^{p^{m-1}} \in \langle a\rangle \cap \langle b\rangle = \{e\}$. This is a contradiction as $|\,a\,| = p^m$, hence $|\,\overline{a}\,| = p^m$. That is, $\overline{a}$ is an element of maximum order in $|\,G\,|$.

As $\left|\,\overline{G}\,\right| < |\,G\,|$, we can use the induction hypothesis to get

$$\overline{G} = \langle \overline{a}\rangle \times \overline{K},$$

for some subgroup $\overline{K}$ of $\overline{G}$.

Let $K = \{x \in G \mid \overline{x} \in \overline{K}\}$. We will show that $G = \langle a\rangle \times K$.

Let $x \in \langle a\rangle \cap K$, then $\overline{x} \in \langle \overline{a}\rangle \cap \overline{K} = \{\overline{e}\} = \{\langle b\rangle\}$. Hence $x \in \langle b\rangle$, but as $x \in \langle a\rangle$, we have $x = e$.

Now, $|\,\langle a\rangle K\,| = |\,\langle a\rangle\,|\,|\,K\,| = |\,\overline{a}\,|\,\left|\,\overline{K}\,\right| p = \left|\,\overline{G}\,\right| p = |\,G\,|$ so that indeed $G = \langle a\rangle \times K$. □

Lemma 11.2.2 and induction gives the following lemma.

Lemma 11.2.3. *A finite Abelian group of prime-power order is an internal direct product of cyclic groups.*

Hence altogether we have proved that

$$G = G(p_1) \times \cdots \times G(p_n),$$

and that each $G(p_i)$ is an internal direct product of cyclic groups. Hence G is an internal direct product of cyclic groups of prime-power order. We are left to show the uniqueness of the direct product obtained above.

The groups $G(p_i)$ are uniquely determined by G as they contain those elements of G whose orders are powers of p_i. We are left to prove that there is only one way (up to isomorphism) to write each $G(p_i)$ as an internal direct product of cyclic subgroups.

Lemma 11.2.4. *Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times \cdots \times H_m$ and $G = K_1 \times \cdots \times K_n$, where the H_i-s and K_i-s are nontrivial cyclic subgroups with $|\,H_1\,| \geq \cdots \geq |\,H_m\,|$ and $|\,K_1\,| \geq \cdots \geq |\,K_n\,|$, then $m = n$ and $|\,H_i\,| = |\,K_i\,|$ for each i.*

Proof. The proof is by induction on $|\,G\,|$. If $|\,G\,| = p$, the result is true. Suppose the statement is true for all Abelian groups of order less than $|\,G\,|$.

For any group L let $L^p = \{x^p \mid x \in L\}$. Then L^p is a subgroup of L (verify this). Further, if p divides the order of L, then by Cauchy's theorem, L has an element of order p, say a.

Hence $a \neq e, a^p = e$, so that the map $a \mapsto a^p$ is not injective, and L^p is a *proper* subgroup of L.

Now $G^p = H_1^p \times \cdots \times H_{m'}^p$ and $G^p = K_1^p \times \cdots \times K_{n'}^p$, where m' is the largest integer i such that $|\, H_i \,| > p$ and n' is the largest integer j such that $|\, K_j \,| > p$ (this is to ensure that the direct product decomposition of G^p does not have trivial factors). By the induction hypothesis, since $|\, G^p \,| < |\, G \,|$, we have $m' = n'$ and $|\, H_i^p \,| = |\, K_i^p \,|$ for all $i = 1, \ldots, m'$. Note that $|\, H_i \,| = |\, H_i^p \,| p$ (Why? Use the fact that H_i is cyclic and that the map $H_i \ni a \to a^p$ has kernel $\{x \in H_i \mid x^p = e\}$). Hence it follows that $|\, H_i \,| = |\, K_i \,|$ for all $i = 1, \ldots, m'$. For the remaining i, $|\, H_i \,| = p = |\, K_i \,|$.

Finally, since $|\, H_i \,| \cdots |\, H'_m \,| p^{m-m'} = |\, G \,| = |\, K_i \,| \cdots |\, K'_n \,| p^{n-n'}$, we have $m - m' = n - n'$, so that $m = n$. □

We have now proved the fundamental theorem, and we restate it.

Theorem. *Every finite Abelian group is a direct product of cyclic groups of prime-power order. Hence G is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$, where the p_i-s are not necessarily distinct, and the prime-powers $p_1^{n_1}, \ldots, p_k^{n_k}$ are uniquely determined by G.*

References

[1] Chapter 11. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.