MATH 369 Fall 2025 - Class Notes

9/29/2025

Scribe: Nick Walden

Summary: We saw that the fundamental theorem of arithmetic can be used to decompose $\mathbb{Z}_n$ into an isomorphic direct product [Topic 1]. We then used that decomposition to find that number of generators of $\mathbb{Z}_n = \varphi(n)$ [Topic 2]. We explored Permutation groups by looking at Cayley's Theorem and Alternating Groups [Topic 3].

Preface: Before we begin, recall that $xy = \text{lcm}(x, y) \cdot \gcd(x, y)$. Also note that brackets may occasionally be omitted and $[a]_n$ may be written as a if it does not significantly detract from clarity.

Topic 1: Direct product decomposition of additive groups of integers.

Theorem 1. $\gcd(m, n) = 1 \implies \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

We will first demonstrate **Proposition 1** about coprime m, n:

$$(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n \implies |(a, b)| = \text{lcm}(|[a]_m|, |[b]_n|)$$

Let l be the least positive integer such that $l([a]_m, [b]_n) = ([0]_m, [0]_n)$. We can see that $l([a]_m, [b]_n) = ([la]_m, [lb]_n)$. Therefore, $la \equiv 0 (\text{mod } m)$ and $lb \equiv 0 (\text{mod } n)$. This means that l is a multiple of $|[a]_m|$ and of $|[b]_n|$. Next, we must show that l is in fact the least common multiple by demonstrating that the lcm always works. If $L = \text{lcm}(|[a]_m|, |[b]_n|)$, we can see that $La \equiv 0 (\text{mod } m)$ and $Lb \equiv 0 (\text{mod } n)$, so $L([a]_m, [b]_n) = ([0]_m, [0]_n)$, $\therefore$ Proposition 1

A good example to build intuition is to think about the order of $(4, 2) \in \mathbb{Z}_{12} \times \mathbb{Z}_4$. When computing the consecutive multiples $k(4, 2)$, we can see that the first k that gives $k(4, 2) = (0, 0) = e$ is $k = 6$, so it has an order of 6. We can also easily see that $\text{lcm}(|[4]_{12}|, |[2]_4|) = \text{lcm}(3, 2) = 6$, which also gives us an order of 6.

Now we are ready to prove Theorem 1. Since we are looking to prove that two groups are isomorphic, we need to look for an isomorphism between them. In order to do this, we will use the fact that both groups are cyclic and have generators $\mathbb{Z}_m \times \mathbb{Z}_n =< ([1]_m, [1]_n) >$ and $\mathbb{Z}_{mn} =< [1]_{mn} >$ and the fact that $| < ([1]_m, [1]_n) > | = | < [1]_{mn} > |$. This allows us to map from one group to the other by mapping $k[1]_{mn}$ to $k([1]_m, [1]_n)$

Proof. Formally, we do this by defining $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ such that $\phi([a]_{mn}) = ([a]_m, [a]_n)$. We will show ϕ is a bijection that satisfies the isomorphism property. We did not explicitly show that the function was well defined in class, but it is trivial to see that it is.

Surjectetive (Onto): Since $|(1, 1)| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$, we know that $(1, 1)$ is a generator, so each element of $\mathbb{Z}_m \times \mathbb{Z}_n$ can be expressed as $k(1, 1)$ for some k. $\phi(k) = (k, k) = k(1, 1)$

Injective (1-1): Suppose $\phi([a]_{mn}) = \phi([b]_{mn})$. Then $([a]_m, [a]_n) = ([b]_m, [b]_n)$, so $a([1]_m, [1]_n) = b([1]_m, [1]_n)$. We can use cancellation to show $(a - b)([1]_m, [1]_n) = ([0]_m, [0]_n)$, so $(a - b) = k \cdot |([1]_m, [1]_n)| = kmn$, so $a \equiv b (\text{mod } mn)$, so $[a]_{mn} = [b]_{mn}$.

Homomorphism: $\phi([a]_{mn}+[b]_{mn}) = \phi([a+b]_{mn}) = ([a+b]_m, [a+b]_n) = ([a]_m+[b]_m, [a]_n+[b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n) = \phi([a]_{mn}) + \phi([b]_{mn})$

Therefore, Theorem 1 is true. □ □

We started building intuition about the implications of Theorem 1 by playing with ways to decompose $\mathbb{Z}_{60}$. We saw that by factorizing 60 we could find several ways to do so including $\mathbb{Z}_4 \times \mathbb{Z}_{15}$, $\mathbb{Z}_5 \times \mathbb{Z}_{12}$, and $\mathbb{Z}_3 \times \mathbb{Z}_{20}$. However, we noted that not all factor pairs work; $\mathbb{Z}_2 \times \mathbb{Z}_{30}$ isn't valid since $\gcd(2, 30) \neq 1$. We saw that we could further break our valid decompositions down; $\mathbb{Z}_4 \times \mathbb{Z}_{15} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ since $15 = 3 \cdot 5$ and $\gcd(3, 5) = 1$.

From there, it's easy to see how we can use the fundamental theorem of arithmetic to decompose any $\mathbb{Z}_n$ into the direct product of some number of prime power moduli:

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times ... \times \mathbb{Z}_{p_k^{e_k}}$$

. Note: If n is a prime power the direct product decomposition is trivial; $\mathbb{Z}_n = \mathbb{Z}_n \times \mathbb{Z}_1$

Topic 2: The **Euler-Phi-Function**: $\varphi(n)$.

Theorem 2. *The number of generators of* $\mathbb{Z}_n = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1}) = \varphi(n)$

We've already seen that $\mathbb{Z}_p$ has $p-1$ generators when p is prime, since $\mathbb{Z}_p$ has p elements and all of them will generate the group except for the identity; $[0]_p$. How many generators does $\mathbb{Z}_{p^f}$ have? $\mathbb{Z}_{p^f}$ has p^f elements, but p^{f-1} of those elements that won't generate the group (all multiples of p and only multiples of p will have gcd $\neq 1$ with p^f, and there are p^{f-1} multiples of p since $p^f/p = p^{f-1}$). Therefore, $\mathbb{Z}_{p^f}$ has $p^f - p^{f-1}$ generators.

When we combine this insight with the FTA prime power decomposition, we arrive at our second theorem. If this is not obvious, consider that $(a_0, a_1, ..., a_k)$ is a generator iff each a_i is a generator of its respective prime power modulus, and we have $p_i^{e_i} - p_i^{e_i-1}$ generator choices for each a_i. For each of the $c_0 = p_0^{e_0} - p_0^{e_0-1}$ options for a_0, we can pick any one of the $c_1 = p_1^{e_1} - p_1^{e_1-1}$ options for a_1, for a total of $c_0 \cdot c_1$ combinations. And for each of those combinations, we can pick any of the c_2 options for a_2, and so on, so we need to find the product of the number of generators of each group.

Topic 3: Permutation Groups

H is a **Permutation Group** if H is a subgroup of a symmetric group S_n. Recall that D_4, the rigid motions of a square, is a subgroup of S_4, so D_4 is a permutation group.

Cayley's Theorem. *Every finite group is isomorphic to a permutation group.*

This means we have essentially already talked about lots of permutation groups (since every finite group we've used in an example has the same properties as some permutation group).

The full proof of Cayley's Theorem is not very quick so instead of rigorously proving all of it we outlined a loose sketch of the proof and focused on really understanding the key idea.

To set up the proof, we suppose G is a finite group. We will look for a subgroup of the symmetric group on G, $S(G)$, which is the group made of all possible permutations of G. To do this, for each $g \in G$, we define $\lambda_g \in S(G)$ by $\lambda_g(h) = gh$. We will then claim that $g \to \lambda_g$ is an isomorphism from G to its image in $S(G)$.

The **key idea** is that since λ_g is multiplication on the left by g, we can think of λ_g as row g of the Cayley table of G (since that's where all the elements of G are multiplied on the left by g), and each row in a Cayley table can be thought of as one line notation for a permutation of the elements of G. In this way, we can naturally assign each element of G to a unique permutation of G

To illustrate this key idea, consider the example $\mathbb{Z}_2 \times \mathbb{Z}_2$. If we list the elements $\{(0,0),(1,0),(0,1),(1,1)\}$, then $\lambda_{(1,0)} = (1,0)+(0,0),(1,0)+(1,0),(1,0)+(0,1),(1,0)+(1,1) = (1,0),(0,0),(1,1),(0,1)$.

Showing that we have a bijection is easy. We've defined the codomain as the image (onto), and, since e is clearly in a different column for each row of the Cayley table, we know that no two rows are the same (1-1). Showing that this is a homomorphism is a bit more tedious and was not covered in class, but it is not particularly hard.

We defined the **Alternating Group** A_n as the set of all even permutations of S_n. Since half of all permutations in S_n can be written as an even number of transpositions, and since $|S_n| = n!$, $|A_n| = \frac{n!}{2}$.

We looked at A_4 to build intuition. $|A_4| = 12$, and when we list all the permutations in A_4 we see that we have:

- One element of order 1: the identity permutation, ()
- Three elements of order 2: the three possible pairs of disjoint transpositions
- Eight elements of order 3: the eight 3-cycles that leave exactly one element fixed, since $(a,b,c) = (a,c)(a,b)$

We played around with different ways we could combine those elements into subgroups, and we started to hypothesize that just because Lagrange's Theorem allows for a subgroup of A_4 with order 6 doesn't necessarily mean we can find one (in other words, the converse of Lagrange's Theorem is false). Instead of tediously checking every possible combination of elements to ensure no subgroup of order 6 exists, we started thinking about how we might prove that such a subgroup doesn't exist, but the proof itself requires first proving a non-trivial proposition and then exploring multiple cases, so the proof was left for a future class.