Math 3230 Abstract Algebra I
Sec 4.4: Finitely generated abelian groups

Slides created by M. Macauley, Clemson (Modified by E. Gunawan, UConn)

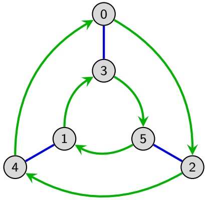
http://egunawan.github.io/algebra

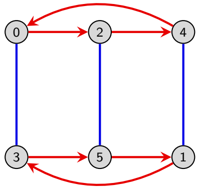
Abstract Algebra I

Finite abelian groups

We've seen that some cyclic groups can be expressed as a direct product of two nontrivial groups, and others cannot.

Below are two ways to lay out the Cayley diagram of $\mathbb{Z}_6$ so the direct product structure is obvious: $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.





However, the group $\mathbb{Z}_8$ *cannot* be written as a direct product of two nontrivial groups. No matter how we draw the Cayley graph, there *must* be an arrow of order 8. (Why?)

We will answer the question of when $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, and in doing so, completely classify all finite abelian groups.

Finite abelian groups

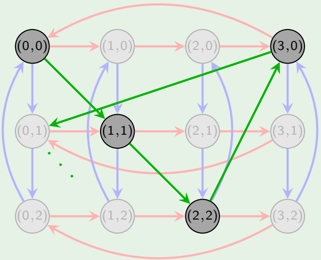
Proposition 1

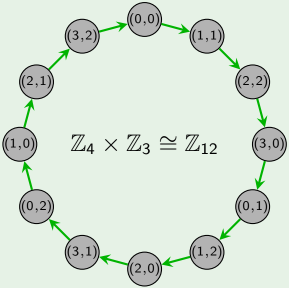
$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if and only if $\gcd(n, m) = 1$.

Proof (sketch)

"$\Leftarrow$": Suppose $\gcd(n, m) = 1$. We claim that $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ has order nm.

To prove the claim, let k denote the order of the element $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Then $(k, k) = (0, 0)$. This means $n \mid k$ and $m \mid k$. In fact, k is $\mathrm{lcm}(n, m)$ the smallest common multiple of n and m. Since n and m has no common divisor, $\mathrm{lcm}(n, m) = nm$. So $k = nm$. ✓





Finite abelian groups

Proposition 1

$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if an only if $\gcd(n, m) = 1$.

Proof (cont.)

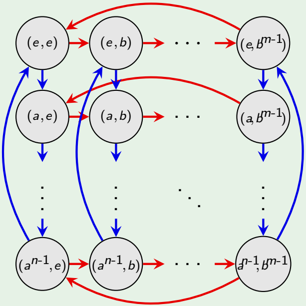
"$\Rightarrow$": Suppose $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an element (a, b) of order nm.

For convenience, we will switch to "multiplicative notation", and denote our cyclic groups by C_n.

Clearly, $\langle a \rangle = C_n$ and $\langle b \rangle = C_m$. Let's look at a Cayley diagram for $C_n \times C_m$.

The order of (a, b) must be a multiple of n (the number of rows), *and* of m (the number of columns).

By definition, this is the *least* common multiple of n and m.



But $|(a, b)| = nm$, and so $\operatorname{lcm}(n, m) = nm$. Therefore, $\gcd(n, m) = 1$. $\square$

The Fundamental Theorem of Finite Abelian Groups

Classification theorem of finite abelian groups (by "prime powers")

Every finite abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $n_1, n_2, \ldots, n_j$,

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_j} \,,$$

where each n_i is a prime power, i.e., $n_i = p_i^{d_i}$, where p_i is prime and $d_i \in \mathbb{N}$.

The proof of this is more advanced, and while it is at the undergraduate level, we don't yet have the tools to do it.

However, we will be more interested in understanding and utilizing this result.

Example

Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$:

$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

The Fundamental Theorem of Finite Abelian Groups

Finite abelian groups can be classified by their "elementary divisors." The mysterious terminology comes from the theory of modules (a graduate-level topic).

Classification theorem (by "elementary divisors")

Every finite abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $k_1, k_2, \dots, k_m$,

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}.$$

where each k_i is a multiple of k_{i+1}.

Example

Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$:

by "prime-powers"	by "elementary divisors"
$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{200}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{100} \times \mathbb{Z}_2$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{40} \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$

The Fundamental Theorem of Finitely Generated Abelian Groups

Just for fun, here is the classification theorem for all *finitely generated* abelian groups. Note that it is not much different.

Theorem

Every finitely generated abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $n_1, n_2, \dots, n_j$,

$$A \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{k \text{ copies}} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_j} ,$$

where each n_i is a prime power, i.e., $n_i = p_i^{d_i}$, where p_i is prime and $d_i \in \mathbb{N}$.

In other words, A is isomorphic to a (multiplicative) group with presentation:

$$A = \langle a_1, \dots, a_k, r_1, \dots, r_m \mid r_i^{n_i} = 1,\ a_i a_j = a_j a_i,\ r_i r_j = r_j r_i,\ a_i r_j = r_j a_i \rangle .$$

In summary, (finitely generated) abelian groups are relatively easy to understand.

In contrast, nonabelian groups are much more mysterious and complicated. The study of *Sylow Theorems* can help us better understand the structure of finite nonabelian groups.