Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

In this video, we discuss an amazing result which gives us a standard form for every finite abelian group.

If $(G,\cdot)$ and $(H,*)$ are two groups, componentwise multiplication gives us a group structure on $G\times H$: $(g_1,h_1)\cdot(g_2,h_2):=(g_1\cdot g_2, h_1 * h_2)$. Since multiplication is done for each component separately, $G\times H$ is an abelian group exactly when G and H are abelian. Based on this and using finite cyclic groups $\mathbb{Z}_n$, we get a family of finite abelian groups: $\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$.

By the Chinese Remainder Theorem, some of these groups are isomorphic to each other: $\mathbb{Z}_m\times\mathbb{Z}_n\simeq\mathbb{Z}_{mn}$ if $\gcd(m,n)=1$.

The amazing result is that every finite abelian group A is of this form. Moreover there are unique integers

$$n_1 \mid n_2 \mid \cdots \mid n_k$$

such that $A\simeq\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}^{(*)}$. We call $(*)$ the standard form of A. We are not going to prove this amazing result. But

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

We see some examples or results related to standard form of abelian groups.

Ex. $\mathbb{Z}_n \times \mathbb{Z}_m$ is not cyclic if $\gcd(m,n) \neq 1$.

Pf Suppose $\gcd(m,n) = d$. Then $\frac{mn}{d} = \left(\frac{m}{d}\right)n = m\left(\frac{n}{d}\right)$ is a common multiple of m and n. Hence for every a, b,

$$\frac{mn}{d}\left([a]_n, [b]_m\right) = \left(n\tfrac{m}{d}[a]_n,\ m\tfrac{n}{d}[b]_m\right) = \left([0]_n, [0]_m\right).$$

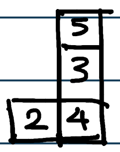
Therefore order of every element of $\mathbb{Z}_n \times \mathbb{Z}_m$ is at most $\frac{mn}{d} < mn$. Hence $\mathbb{Z}_n \times \mathbb{Z}_m$ has no element of order $mn = |\mathbb{Z}_n \times \mathbb{Z}_m|$. Therefore $\mathbb{Z}_n \times \mathbb{Z}_m$ is not cyclic. ∎

Ex. Find the standard form of $\mathbb{Z}_{12} \times \mathbb{Z}_{10}$.

Solution. We use the CRT to break them apart and reconnect them in a different order!

$$\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \quad \text{and} \quad \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5.$$

$$\Rightarrow \mathbb{Z}_{12} \times \mathbb{Z}_{10} \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4}_{\text{powers of } 2} \times \underbrace{\mathbb{Z}_3}_{\text{powers of } 3} \times \underbrace{\mathbb{Z}_5}_{\text{powers of } 5}$$



$$\simeq \mathbb{Z}_2 \times \mathbb{Z}_{4\cdot 3\cdot 5} = \mathbb{Z}_2 \times \mathbb{Z}_{60} \quad \text{(Notice } 2 \mid 60\text{)}$$

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

Ex. Find the standard form of $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_{45}$.

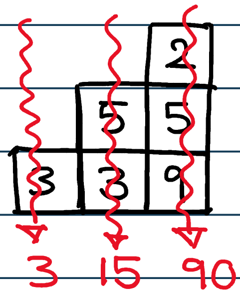
Solution. Step 1. Factoring to primes and using CRT

$\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_{45} \simeq \mathbb{Z}_9 \times \mathbb{Z}_5$.

Step 2. Regrouping in terms of prime factors

$$\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_{45} \simeq \underbrace{\mathbb{Z}_2}_{2} \times \underbrace{\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9}_{3} \times \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_5}_{5}$$

Step 3. Creating a "building" using existing "blocks of prime powers"



Step 4. Multiply each column.

$$\begin{aligned}\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_{45} \simeq\ & \mathbb{Z}_3 \times \\ & (\mathbb{Z}_5 \times \mathbb{Z}_3) \times \\ & (\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9) \\ \simeq\ & \mathbb{Z}_3 \times \mathbb{Z}_{15} \times \mathbb{Z}_{90}.\end{aligned}$$

Ex. Find the standard form of $\mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \mathbb{Z}_{30}$.

Solution. Step 1. Factoring to primes

$\mathbb{Z}_{20} \simeq \mathbb{Z}_4 \times \mathbb{Z}_5$, $\mathbb{Z}_{50} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{25}$, $\mathbb{Z}_{30} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Finite abelian groups

Tuesday, June 29, 2021   3:29 PM

<u>Step 2.</u> Reordering in terms of primes.

$$\mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \mathbb{Z}_{30} \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4}_{2} \times \underbrace{\mathbb{Z}_3}_{3} \times \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}}_{5}$$

<u>Step 3.</u> Creating a "building" using existing "blocks of prime powers"

		3
5	5	25
2	2	4

<u>Step 4.</u> Multiplying columns (and using CRT)

$$\mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \mathbb{Z}_{30} \simeq (\mathbb{Z}_5 \times \mathbb{Z}_2) \times (\mathbb{Z}_5 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_4)$$

$$\simeq \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{300} \qquad \blacksquare$$

Next we see how we can use the 1st isomorphism theorem to find the standard form of an abelian group which is given as a quotient group.

<u>Ex.</u> Find the standard form of $\mathbb{Z} \times \mathbb{Z} / \langle (2,0), (0,5) \rangle$.

In general one needs to use Smith form of integer matrices to answer this type of questions. Here we illustrate some basic

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

examples.

Consider the group homomorphism $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_5$,

$f(a,b) := ([a]_2, [b]_5)$ (Check why it is a group homomorphism)

Clearly f is surjective. Next we find its kernel.

$$(a,b) \in \ker f \iff [a]_2 = [0]_2 \text{ and } [b]_5 = [0]_5$$

$$\iff a = 2r \text{ and } b = 5s \text{ for some } r, s \in \mathbb{Z}.$$

$$\iff (a,b) = r(2,0) + s(0,5)$$

Therefore $\ker f = \{ r(2,0) + s(0,5) \mid r, s \in \mathbb{Z} \}$.

Claim. $\ker f = \langle (2,0), (0,5) \rangle$.

Pf of Claim. $(2,0) = 1 \cdot (2,0) + 0 \cdot (0,5) \in \ker f$

$(0,5) = 0 \cdot (2,0) + 1 \cdot (0,5) \in \ker f$

$\Rightarrow \langle (2,0), (0,5) \rangle \subseteq \ker f$. (I)

Since $\langle (2,0), (0,5) \rangle$ is a closed under addition and subtraction $r(2,0) + s(0,5) \in \langle (2,0), (0,5) \rangle$ for every $r, s \in \mathbb{Z}$. $\Rightarrow \ker f \subseteq \langle (2,0), (0,5) \rangle$ (II)

By (I) and (II), Claim follows.

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

By the 1st isomorphism theorem,

$$\mathbb{Z}\times\mathbb{Z}/\ker f \simeq \operatorname{Im} f; \text{ and so } \mathbb{Z}\times\mathbb{Z}/\langle(2,0),(0,5)\rangle \simeq \mathbb{Z}_2\times\mathbb{Z}_5$$

By the CRT, $\mathbb{Z}_2\times\mathbb{Z}_5 \simeq \mathbb{Z}_{10}$; hence

$$\mathbb{Z}\times\mathbb{Z}/\langle(2,0),(0,5)\rangle \simeq \mathbb{Z}_{10}. \quad \blacksquare$$

<u>Remark</u>. By a similar argument one can show that for positive integers m and n,

$$\mathbb{Z}\times\mathbb{Z}/\langle(m,0),(0,n)\rangle \simeq \mathbb{Z}_m\times\mathbb{Z}_n.$$

The next result can help us answer more questions of this type.

<u>Lemma</u>. Suppose $(a_1,b_1),(a_2,b_2)\in\mathbb{Z}\times\mathbb{Z}$ and

$$\det\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2\end{bmatrix} = \pm 1 \quad (\text{i.e. } a_1b_2 - a_2b_1 = \pm 1).$$

Then $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$, $f(m,n) := m(a_1,b_1)+n(a_2,b_2)$ is an automorphism.

<u>Pf.</u> We can write elements of $\mathbb{Z}\times\mathbb{Z}$ as <u>2×1</u> column vectors, and f can be viewed as a matrix multiplication.

$$\begin{bmatrix} m \\ n\end{bmatrix} \xmapsto{f} \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2\end{bmatrix}\begin{bmatrix} m \\ n\end{bmatrix} = \begin{bmatrix} m\,a_1 + n\,a_2 \\ m\,b_1 + n\,b_2\end{bmatrix}.$$

Notice that for every $v, w \in \mathbb{Z}\times\mathbb{Z}$,

$$\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}(v+w) = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix} v + \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix} w,$$

and so f is a group homomorphism.

<u>f is invertible</u>. Recall that inverse of a 2×2 matrix is given as follows:

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}^{-1} = \frac{1}{\det} \begin{bmatrix} x_{22} & -x_{12} \\ -x_{21} & x_{11} \end{bmatrix}$$

Hence if $x_{ij} \in \mathbb{Z}$ and $\det = \pm 1$, then all the entries of $\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}^{-1}$ are in $\mathbb{Z}$. Therefore

$$v \longmapsto \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}^{-1} v$$ is a function from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}\times\mathbb{Z}$

which is the inverse of f. This completes the proof. ∎

Let's see how the above lemma can help us understand structure of some of quotient groups.

<u>Ex.</u> Find the standard form of $\mathbb{Z}\times\mathbb{Z}/\langle 3(2,1), 5(3,2)\rangle$.

<u>Solution.</u> Notice that $\det\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} = 1$ and so

$f: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$, $f(m,n) = m(2,1) + n(3,2)$ is an

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

isomorphism. Consider the group homomorphism

$$\mathbb{Z}\times\mathbb{Z} \xrightarrow{f} \mathbb{Z}\times\mathbb{Z} \xrightarrow{p} \mathbb{Z}\times\mathbb{Z}/\langle 3(2,1),5(3,2)\rangle$$

$$\xrightarrow{\bar{f}}$$

where p is the natural quotient map; this means

$$p(r,s) = (r,s) + \langle 3(2,1), 5(3,2)\rangle$$

Recall that $\ker p = \langle 3(2,1), 5(3,2)\rangle$ and p is surjective.

- Since f and p are surjective, $\bar{f}$ is surjective.
- $(r,s)\in \ker \bar{f} \iff p(f(r,s))$ is zero of $\mathbb{Z}\times\mathbb{Z}/\langle 3(2,1), 5(3,2)\rangle$.

$$\iff f(r,s)\in \ker p$$

$$\iff (r,s) \in f^{-1}(\langle 3(2,1), 5(3,2)\rangle$$

$$\iff (r,s) \in \langle 3\ f^{-1}(2,1), 5\ f^{-1}(3,2)\rangle$$

$$\iff (r,s) \in \langle 3(1,0), 5(0,1)\rangle.$$

- By the 1st isomorphism theorem $\mathbb{Z}\times\mathbb{Z}/_{\ker \bar{f}} \simeq \operatorname{Im} \bar{f}$.

Hence $\mathbb{Z}\times\mathbb{Z}/\langle 3(1,0), 5(0,1)\rangle \simeq \mathbb{Z}\times\mathbb{Z}/\langle 3(2,1),5(3,2)\rangle$.

Similar to the previous example $\mathbb{Z}\times\mathbb{Z}/\langle 3(1,0),5(0,1)\rangle \simeq \mathbb{Z}_3\times\mathbb{Z}_5$.

Finite abelian groups

Tuesday, June 29, 2021 3:29 PM

Altogether

$$\mathbb{Z}\times\mathbb{Z}/\langle 3(2,1),5(3,2)\rangle \simeq \mathbb{Z}\times\mathbb{Z}/\langle 3(1,0),5(0,1)\rangle$$

$$\simeq \mathbb{Z}_3\times\mathbb{Z}_5$$

$$\simeq \mathbb{Z}_{15} \qquad \text{(by the CRT)}.$$